Fraunhofer

Fraunhofer Competence Center PKI

PKI Contacts – PKI for Fraunhofer Contacts

User manual for communication partners of the Fraunhofer-Gesellschaft

Author[s]:

Uwe Bendisch, Maximilian Gottwald

As at: 15.10.2013

Version 1.0

Document history:

VERSION	DATE	MODIFICATIONS	AUTHOR
1.0	23.01.2014	Final review	UB
0.9	15.10.2013	Creation of German version with English screen shots	MG, UB

Mailing list/target group:

This document is aimed at those communications partners of the Fraunhofer-Gesellschaft who wish to use certificate-based authentication to protect their e-mail correspondence with Fraunhofer-Gesellschaft employees and who do not yet possess certificates for the purpose.

Remarks/notes:

This document has been put together with great care and attention to detail, but sadly this does not guarantee the absence of errors. Liability can be accepted neither for any errors that may occur nor for their possible consequences. Please feel free to inform us of any mistakes found in the document or to suggest alterations – if possible in the form of pre-formulated passages of text – by e-mailing the Fraunhofer service desk at servicedesk@fraunhofer.de. We will do our very best to take up every good idea we receive and to implement your suggested improvements.

Internal information:

File name:	PKI-Contacts_Anleitung_Extern_EN (V 1.0).docx
Time:	24.01.2014
Editor:	Uwe Bendisch

Contents

Introduction

This document describes how to establish secure e-mail communications with Fraunhofer-Gesellschaft employees.

In order to establish encrypted e-mail communications, you and the Fraunhofer employee you wish to communicate with must each be in possession of a digital encryption certificate. Fraunhofer employees have for the most part already been provided with encryption certificates.

To ensure you too are able to obtain a certificate for communicating with Fraunhofer, the Fraunhofer-Gesellschaft – or rather its Public Key Infrastructures Competence Center, to be precise – runs its own public key infrastructure (PKI) that is completely separate from the PKI for Fraunhofer Employees. It is called *PKI Contacts* (PKI for Fraunhofer Contacts), and issues certificates to external communications partners of Fraunhofer employees.

You can use certificates issued to you to create signed e-mails, too. Recipients of such e-mails can be certain that the message is actually from you, and that it was not modified during transmission.

Please note that *PKI Contacts* can issue certificates only when prompted to do so by a Fraunhofer-Gesellschaft employee.

Note: Unless otherwise indicated, the screenshots contained in this manual were created using Mozilla Firefox and Thunderbird version 24 in Windows 7. The appearance of individual dialog windows may differ depending on the operating system or browser used. Internal browser processes may also vary slightly from product to product, particularly when it comes to selecting certificates or entering smartcard PINs.

1 Obtaining a Fraunhofer employee's certificate

In order to send a Fraunhofer employee an encrypted e-mail, you need his/her digital encryption certificate. You can receive this certificate by e-mail or download it from this website: https://contacts.pki.fraunhofer.de.

1.1 Receiving a certificate by e-mail

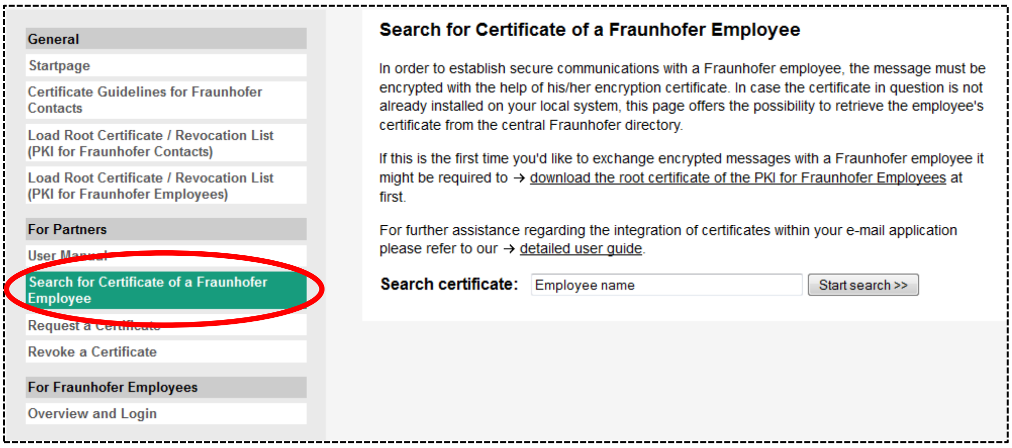
In order to obtain a Fraunhofer employee's digital encryption certificate by e-mail, you need to request that they send you a signed e-mail. Once the root certificates and remaining certificates in the PKI for Fraunhofer Employees certificate chain are integrated correctly into your e-mail client (see chapter 4.1.2), the Fraunhofer employee's certificate will be available for secure communication by e-mail. You can now answer the Fraunhofer employee's e-mail directly with an encrypted e-mail.

Note: The root certificate and the corresponding certificates from the PKI for Fraunhofer Employees certificate chain need to be imported only once into your e-mail program's certificate store.

1.2 Downloading a certificate from the *PKI Contacts* website

If you wish to send an encrypted e-mail to a Fraunhofer employee who already has a valid Fraunhofer PKI certificate that you are not yet in possession of, then you can obtain this certificate from https://contacts.pki.fraunhofer.de.

Open the link in your browser and select **Search Certificate of a Fraunhofer Employee** under the **For Partners** section of the menu (see Figure 1).


General
Startpage
Certificate Guidelines for Fraunhofer Contacts
Load Root Certificate / Revocation List (PKI for Fraunhofer Contacts)
Load Root Certificate / Revocation List (PKI for Fraunhofer Employees)
For Partners
User Manual
Search for Certificate of a Fraunhofer Employee
Request a Certificate
Revoke a Certificate
For Fraunhofer Employees
Overview and Login

Search for Certificate of a Fraunhofer Employee

In order to establish secure communications with a Fraunhofer employee, the message must be encrypted with the help of his/her encryption certificate. In case the certificate in question is not already installed on your local system, this page offers the possibility to retrieve the employee's certificate from the central Fraunhofer directory.

If this is the first time you'd like to exchange encrypted messages with a Fraunhofer employee it might be required to → download the root certificate of the PKI for Fraunhofer Employees at first.

For further assistance regarding the integration of certificates within your e-mail application please refer to our → detailed user guide.

Search certificate: Employee name

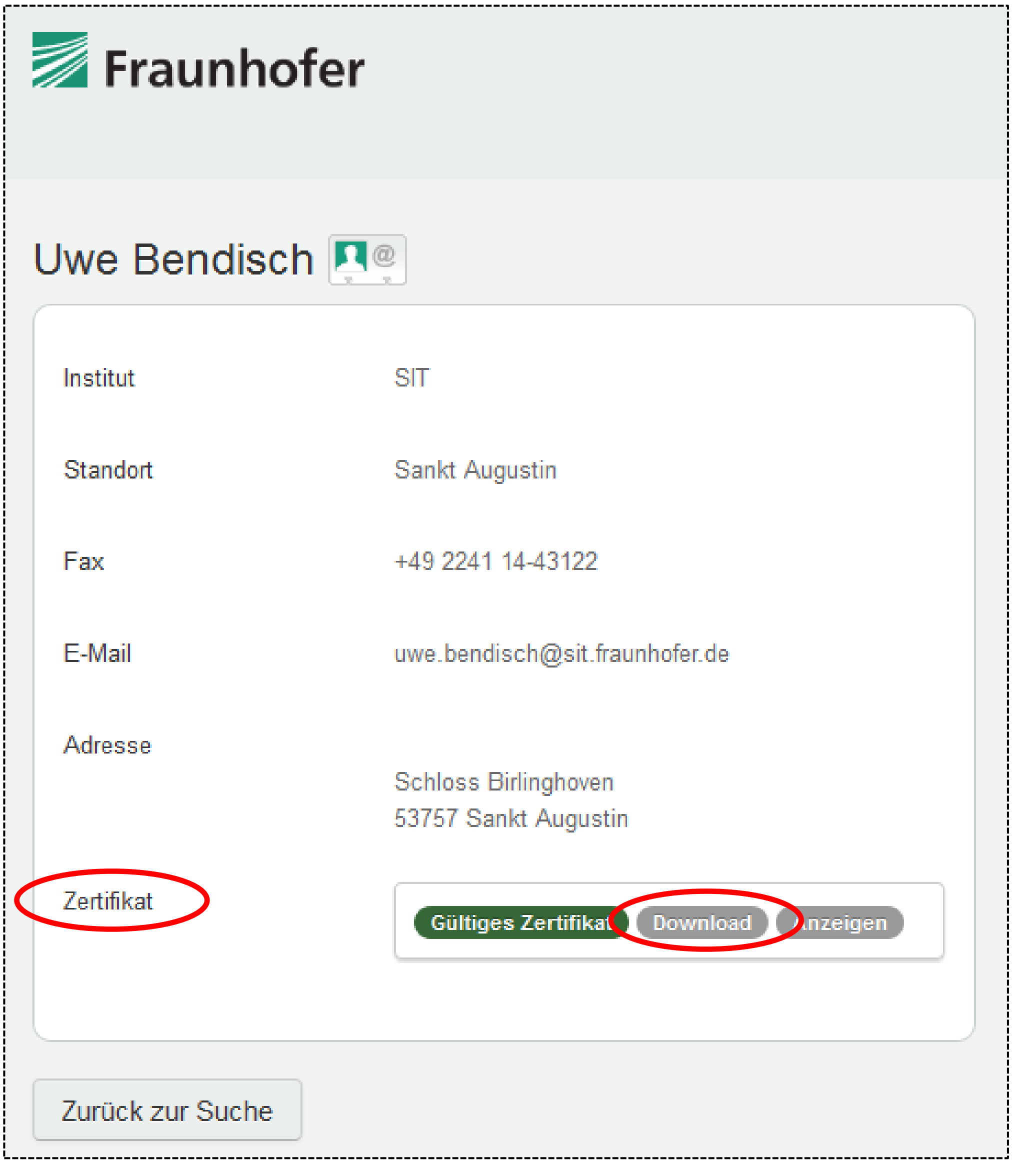
Figure 1: Screen with search field for looking up certificates of Fraunhofer employees

Enter the surname of the Fraunhofer employee whose certificate you wish to obtain and click on **Start search**.

Note: You do not have to enter the whole name. Entering part of the name will produce a list of Fraunhofer employees whose surnames contain the part you searched for.

Note: For reasons of data protection, the number of search results shown is limited to three. Should the Fraunhofer employee you are searching for not be listed, it may be worth refining your search by entering a name/part of a name that contains more letters.

If the search finds a Fraunhofer employee whose name corresponds to the name you entered, you will be presented with a window displaying that employee’s publicly available data as depicted in Figure 2. If this Fraunhofer employee is in possession of a digital encryption certificate, the details are shown in the section entitled “Zertifikat” (*Certificate*).



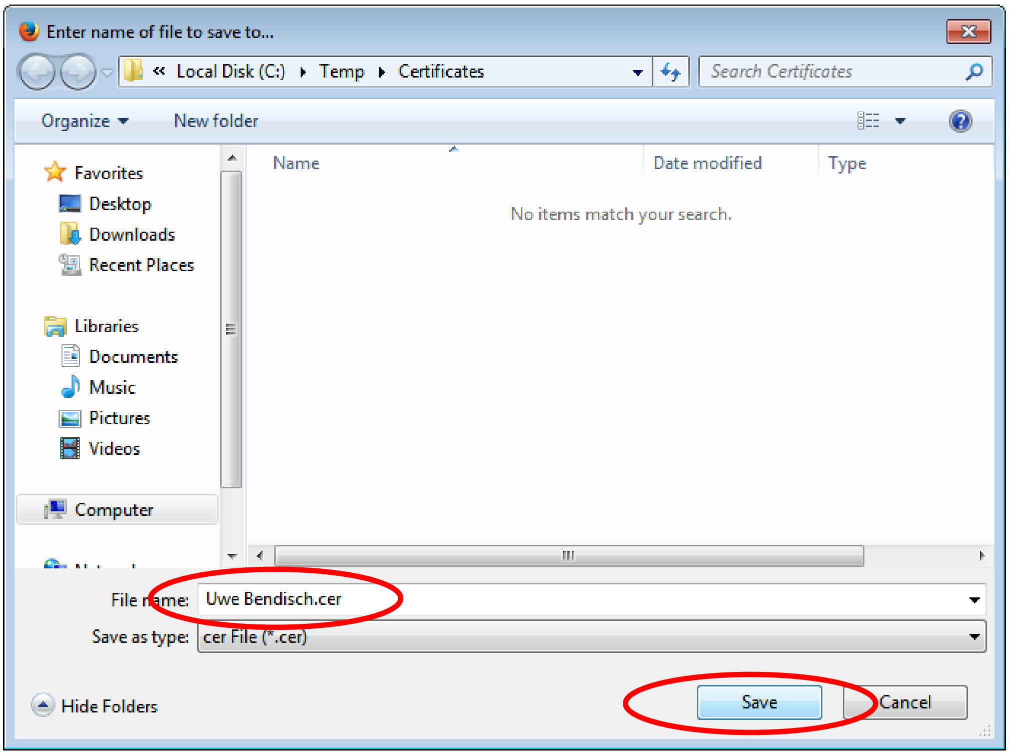
Uwe Bendisch

Institut	SIT
Standort	Sankt Augustin
Fax	+49 2241 14-43122
E-Mail	uwe.bendisch@sit.fraunhofer.de
Adresse	Schloss Birlinghoven 53757 Sankt Augustin
Zertifikat	Gültiges Zertifikat Download Anzeigen

Figure 2: Results of search for a Fraunhofer employee's certificate

To save a valid certificate on your computer, click on **Download** and select the option **Save File**.

Now select the folder in which you want to save the certificate, and click on **Save**. You can replace or change the suggested filename, but please ensure the file extension *.cer* remains unchanged (see Figure 3).



File name: Uwe Bendisch.cer

Save as type: cer File (*.cer)

Figure 3: Saving a Fraunhofer employee’s certificate

The process for integrating certificates into your e-mail client in order to use them for secure communication varies depending on the e-mail client you use. This process is described under section 4.3.

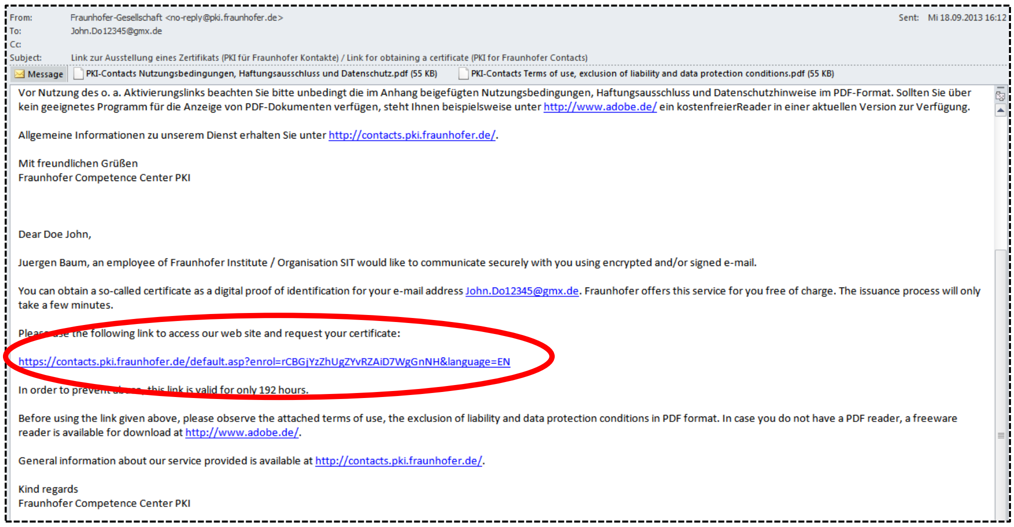
2 Requesting your own personal certificate

In order to establish secure e-mail communications with Fraunhofer you too need a certificate that is assigned to your e-mail address. In case you don't yet have a personal certificate of your own, you can obtain a free one from the PKI for Fraunhofer Contacts, *PKI Contacts*.

Certificates can be issued only once requested by a Fraunhofer employee who knows you. Please ask your contact at Fraunhofer to apply for a certificate on your behalf. It is then up to you to generate a key and request a certificate yourself.

There is a secure part of the website https://contacts.pki.fraunhofer.de with protected access from which Fraunhofer employees can authorize the issuing of certificates for communication partners.

During the course of the process you will receive an automatically generated e-mail containing a link (see Figure 4) that takes you to a special *PKI Contacts* website that leads you through the certificate application process. Click on the link provided in the e-mail or copy the address bar into your browser.



From: Fraunhofer-Gesellschaft <no-reply@pki.fraunhofer.de>
Sent: Mi 18.09.2013 16:12
To: John.Do12345@gmx.de
Cc:
Subject: Link zur Ausstellung eines Zertifikats (PKI für Fraunhofer Kontakte) / Link for obtaining a certificate (PKI for Fraunhofer Contacts)

Message
PKI-Contacts Nutzungsbedingungen, Haftungsausschluss und Datenschutz.pdf (55 KB)
PKI-Contacts Terms of use, exclusion of liability and data protection conditions.pdf (55 KB)

Vor Nutzung des o. a. Aktivierungslinks beachten Sie bitte unbedingt die im Anhang beigefügten Nutzungsbedingungen, Haftungsausschluss und Datenschutzhinweise im PDF-Format. Sollten Sie über kein geeignetes Programm für die Anzeige von PDF-Dokumenten verfügen, steht Ihnen beispielsweise unter http://www.adobe.de/ ein kostenfreierReader in einer aktuellen Version zur Verfügung.

Allgemeine Informationen zu unserem Dienst erhalten Sie unter http://contacts.pki.fraunhofer.de/.

Mit freundlichen Grüßen
Fraunhofer Competence Center PKI

Dear Doe John,

Juergen Baum, an employee of Fraunhofer Institute / Organisation SIT would like to communicate securely with you using encrypted and/or signed e-mail.

You can obtain a so-called certificate as a digital proof of identification for your e-mail address John.Do12345@gmx.de. Fraunhofer offers this service for you free of charge. The issuance process will only take a few minutes.

Please use the following link to access our web site and request your certificate:

https://contacts.pki.fraunhofer.de/default.asp?enrol=rCBGjYzZhUgZYvRZAiD7WgGnNH&language=EN

In order to prevent abuse, this link is valid for only 192 hours.

Before using the link given above, please observe the attached terms of use, the exclusion of liability and data protection conditions in PDF format. In case you do not have a PDF reader, a freeware reader is available for download at http://www.adobe.de/.

General information about our service provided is available at http://contacts.pki.fraunhofer.de/.

Kind regards
Fraunhofer Competence Center PKI

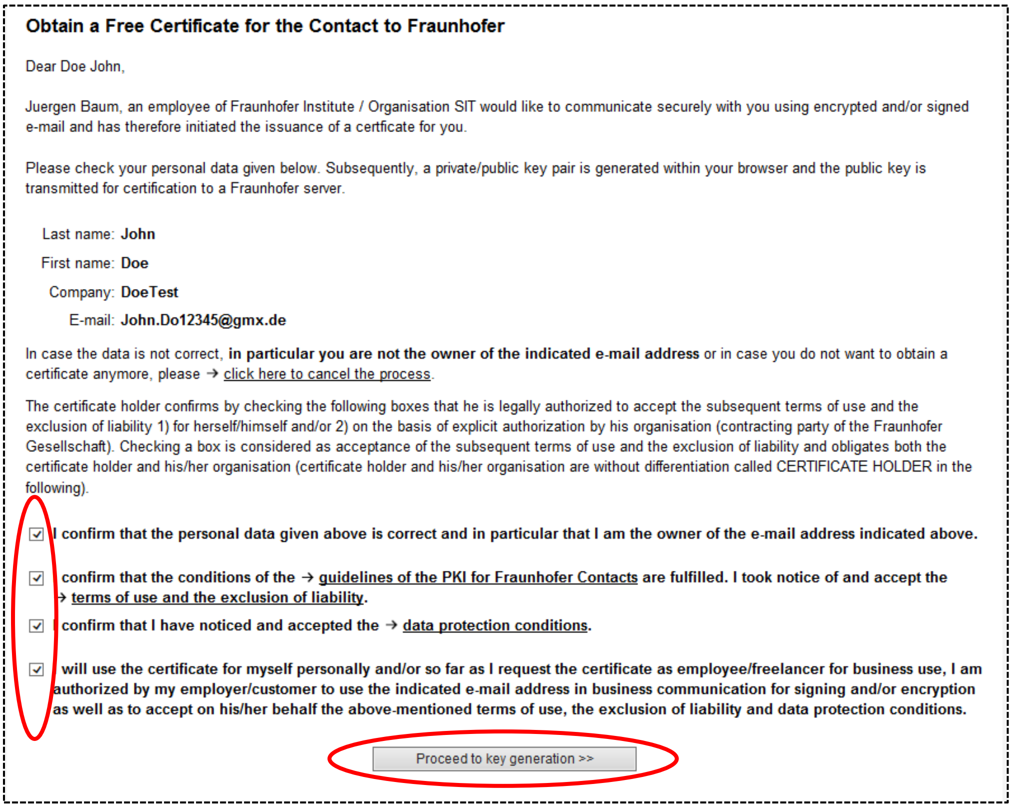
Figure 4: E-mail with link for issuing a certificate

Note: Please be aware that for security reasons the link contains an identification feature that is valid only for you. Furthermore, the link must be used within 192 hours of the e-mail being sent. If you do not apply for a certificate within this time, you must ask your contact at the Fraunhofer-Gesellschaft to make a new request for authorization on your behalf.

2.1 Requesting your own personal certificate with Microsoft Internet Explorer

Note: Screenshots were created using Microsoft Internet Explorer version 10.

The link contained in the automatically generated e-mail takes you to a website that leads you through the certificate application process (see Figure 5).



Obtain a Free Certificate for the Contact to Fraunhofer

Dear Doe John,

Juergen Baum, an employee of Fraunhofer Institute / Organisation SIT would like to communicate securely with you using encrypted and/or signed e-mail and has therefore initiated the issuance of a certficate for you.

Please check your personal data given below. Subsequently, a private/public key pair is generated within your browser and the public key is transmitted for certification to a Fraunhofer server.

Last name:	**John**
First name:	**Doe**
Company:	**DoeTest**
E-mail:	**John.Do12345@gmx.de**

In case the data is not correct, **in particular you are not the owner of the indicated e-mail address** or in case you do not want to obtain a certificate anymore, please → click here to cancel the process.

The certificate holder confirms by checking the following boxes that he is legally authorized to accept the subsequent terms of use and the exclusion of liability 1) for herself/himself and/or 2) on the basis of explicit authorization by his organisation (contracting party of the Fraunhofer Gesellschaft). Checking a box is considered as acceptance of the subsequent terms of use and the exclusion of liability and obligates both the certificate holder and his/her organisation (certificate holder and his/her organisation are without differentiation called CERTIFICATE HOLDER in the following).

☑ **I confirm that the personal data given above is correct and in particular that I am the owner of the e-mail address indicated above.**

☑ **I confirm that the conditions of the → guidelines of the PKI for Fraunhofer Contacts are fulfilled. I took notice of and accept the → terms of use and the exclusion of liability.**

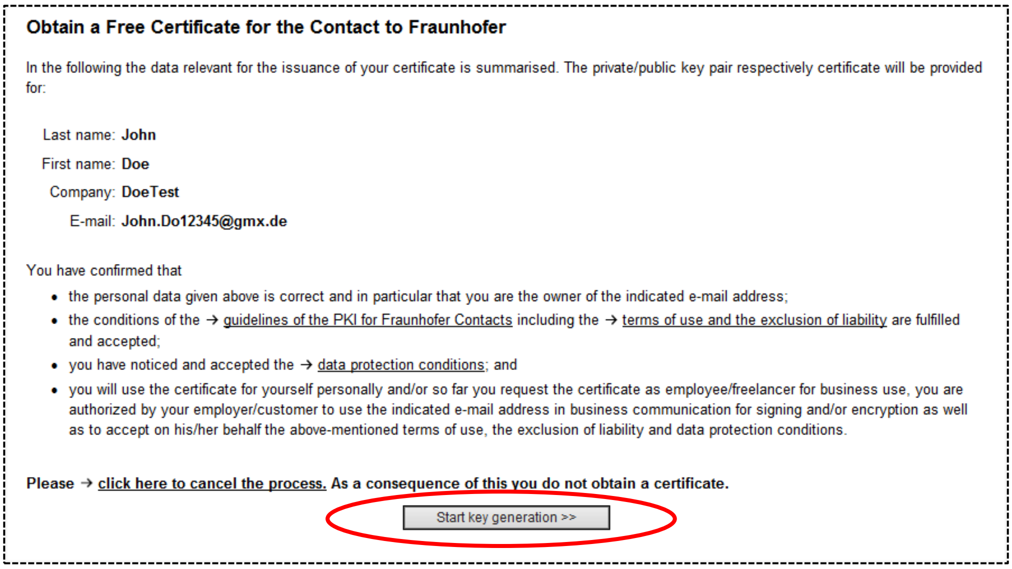
☑ **I confirm that I have noticed and accepted the → data protection conditions.**

☑ **I will use the certificate for myself personally and/or so far as I request the certificate as employee/freelancer for business use, I am authorized by my employer/customer to use the indicated e-mail address in business communication for signing and/or encryption as well as to accept on his/her behalf the above-mentioned terms of use, the exclusion of liability and data protection conditions.**

Figure 5: Certificate issuance with Internet Explorer – user's data check and confirmation of having read the guidelines for issuing certificates etc.

Now please check your personal information and confirm that it is correct. Please also confirm that you acknowledge and comply with the remaining specified conditions and disclaimers, in particular confirming that you have understood and will comply with the guidelines for the issuance of certificates of the PKI for Fraunhofer Contacts.

Click **Proceed to key generation** to be presented with a summary of the information you have entered and the confirmations you have given (see Figure 6). You also have the option to cancel the certificate generating process at this stage. Doing so means you will not receive a certificate.



Obtain a Free Certificate for the Contact to Fraunhofer

In the following the data relevant for the issuance of your certificate is summarised. The private/public key pair respectively certificate will be provided for:

Last name: **John**
First name: **Doe**
Company: **DoeTest**
E-mail: **John.Do12345@gmx.de**

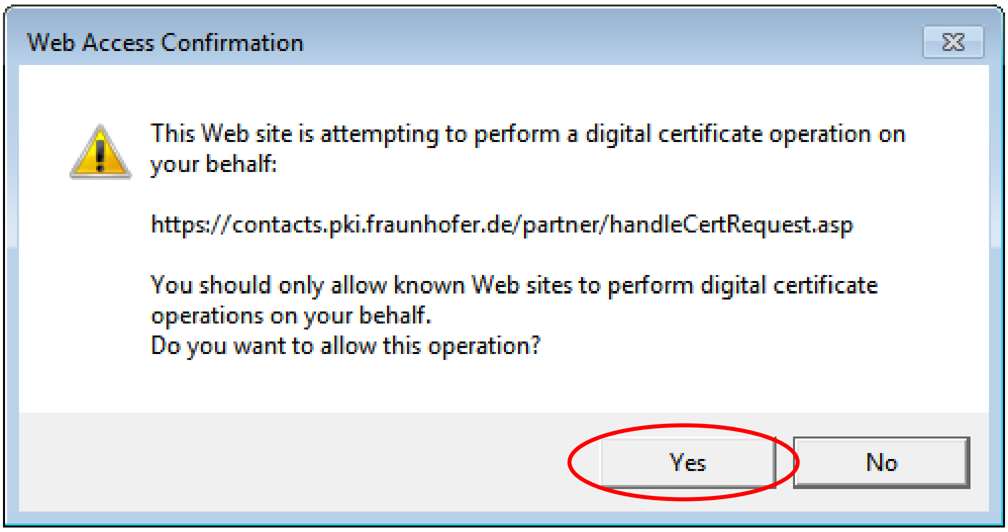
You have confirmed that

- the personal data given above is correct and in particular that you are the owner of the indicated e-mail address;
- the conditions of the → guidelines of the PKI for Fraunhofer Contacts including the → terms of use and the exclusion of liability are fulfilled and accepted;
- you have noticed and accepted the → data protection conditions; and
- you will use the certificate for yourself personally and/or so far you request the certificate as employee/freelancer for business use, you are authorized by your employer/customer to use the indicated e-mail address in business communication for signing and/or encryption as well as to accept on his/her behalf the above-mentioned terms of use, the exclusion of liability and data protection conditions.

Please → click here to cancel the process. As a consequence of this you do not obtain a certificate.

Figure 6: Issuing certificates with Internet Explorer – summary of information entered by the user and the confirmations they have given

Click on **Start key generation** to generate a cryptographic key pair in your browser and to transmit the public key to the web server that will use it to create your certificate. As this is a security-sensitive process, Internet Explorer issues a caution warning you of the security risks involved, and asks you to confirm that you wish to proceed (see Figure 7). Please confirm the security prompt by clicking **Yes** and wait for a moment until the keys have been generated.



Web Access Confirmation

This Web site is attempting to perform a digital certificate operation on your behalf:

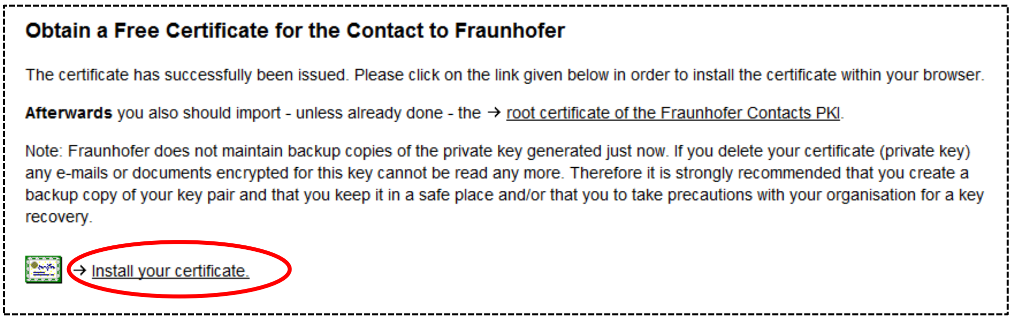
https://contacts.pki.fraunhofer.de/partner/handleCertRequest.asp

You should only allow known Web sites to perform digital certificate operations on your behalf.
Do you want to allow this operation?

Figure 7: Issuing certificates with Internet Explorer – security prompt as part of key-generation process

Once keys and certificate have been generated, you will receive a message that the certificate is ready to be installed. To do so, click on the link **Install your**

certificate (see Figure 8). This installs the certificate in the Internet Explorer certificate store (Microsoft certificate store).



Obtain a Free Certificate for the Contact to Fraunhofer

The certificate has successfully been issued. Please click on the link given below in order to install the certificate within your browser.

Afterwards you also should import - unless already done - the → root certificate of the Fraunhofer Contacts PKI.

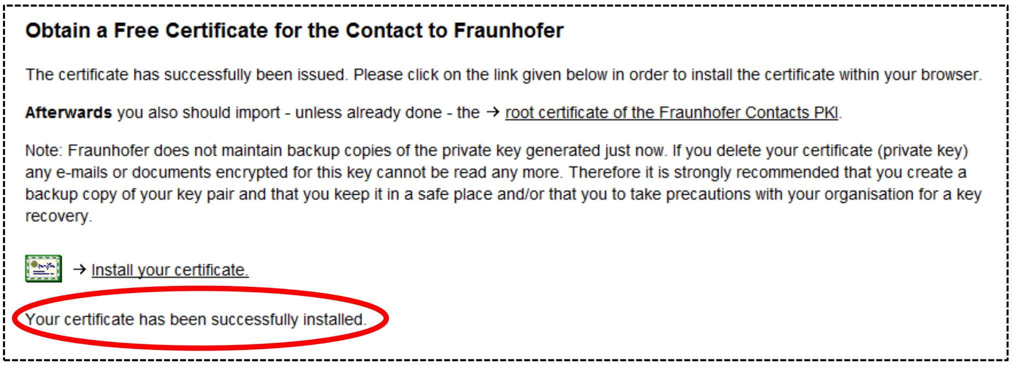
Note: Fraunhofer does not maintain backup copies of the private key generated just now. If you delete your certificate (private key) any e-mails or documents encrypted for this key cannot be read any more. Therefore it is strongly recommended that you create a backup copy of your key pair and that you keep it in a safe place and/or that you to take precautions with your organisation for a key recovery.

→ Install your certificate.

Figure 8: Issuing certificates with Internet Explorer – confirmation that the certificate was successfully issued

Internet Explorer uses the same caution message as shown in Figure 7 to warn you of the potential security risk that installing the certificate poses. Please confirm the security prompt by clicking **Yes**.

You will now receive a message informing you that the certificate has been successfully installed in your browser (see Figure 9).



Obtain a Free Certificate for the Contact to Fraunhofer

The certificate has successfully been issued. Please click on the link given below in order to install the certificate within your browser.

Afterwards you also should import - unless already done - the → root certificate of the Fraunhofer Contacts PKI.

Note: Fraunhofer does not maintain backup copies of the private key generated just now. If you delete your certificate (private key) any e-mails or documents encrypted for this key cannot be read any more. Therefore it is strongly recommended that you create a backup copy of your key pair and that you keep it in a safe place and/or that you to take precautions with your organisation for a key recovery.

→ Install your certificate.

Your certificate has been successfully installed.

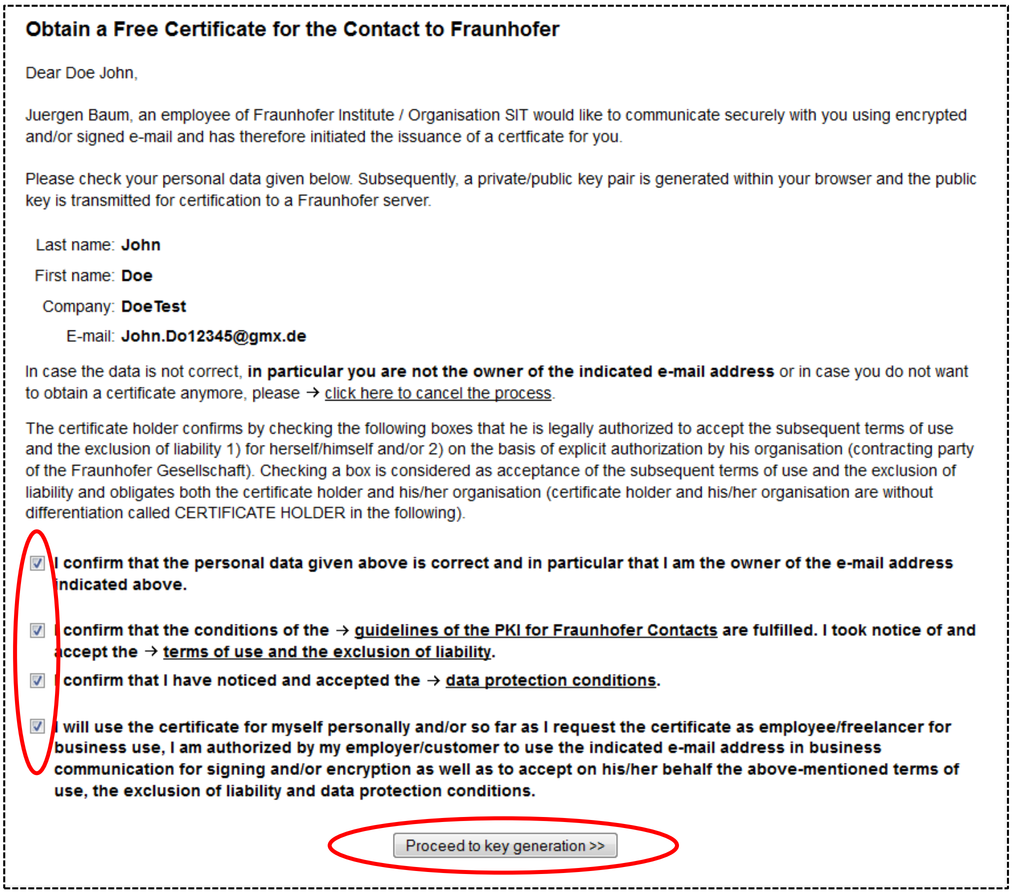
Figure 9: Issuing certificates with Internet Explorer – confirmation that the certificate has been installed

In order to be able to use the certificate in your e-mail client, you may now have to export it from your browser and import it into your e-mail client. This process depends on the type of browser and e-mail client you use. Section 3.1 describes how to export certificates from Internet Explorer, and chapter 0 describes how to use your personal certificate in different e-mail clients.

Note: Please be aware that it is not necessary to export a certificate from Internet Explorer if you intend to use it with an e-mail client that also accesses the Microsoft certificate store (such as Microsoft Outlook). In such cases it is enough to configure the certificate in the e-mail client (see chapter 0).

2.2 Requesting your own personal certificate with Mozilla Firefox

The link contained in the automatically generated e-mail takes you to a website that leads you through the certificate application process (see Figure 10).



Obtain a Free Certificate for the Contact to Fraunhofer

Dear Doe John,

Juergen Baum, an employee of Fraunhofer Institute / Organisation SIT would like to communicate securely with you using encrypted and/or signed e-mail and has therefore initiated the issuance of a cerfticate for you.

Please check your personal data given below. Subsequently, a private/public key pair is generated within your browser and the public key is transmitted for certification to a Fraunhofer server.

Last name:	**John**
First name:	**Doe**
Company:	**DoeTest**
E-mail:	**John.Do12345@gmx.de**

In case the data is not correct, **in particular you are not the owner of the indicated e-mail address** or in case you do not want to obtain a certificate anymore, please → click here to cancel the process.

The certificate holder confirms by checking the following boxes that he is legally authorized to accept the subsequent terms of use and the exclusion of liability 1) for herself/himself and/or 2) on the basis of explicit authorization by his organisation (contracting party of the Fraunhofer Gesellschaft). Checking a box is considered as acceptance of the subsequent terms of use and the exclusion of liability and obligates both the certificate holder and his/her organisation (certificate holder and his/her organisation are without differentiation called CERTIFICATE HOLDER in the following).

☑ **I confirm that the personal data given above is correct and in particular that I am the owner of the e-mail address indicated above.**

☑ **I confirm that the conditions of the → guidelines of the PKI for Fraunhofer Contacts are fulfilled. I took notice of and accept the → terms of use and the exclusion of liability.**

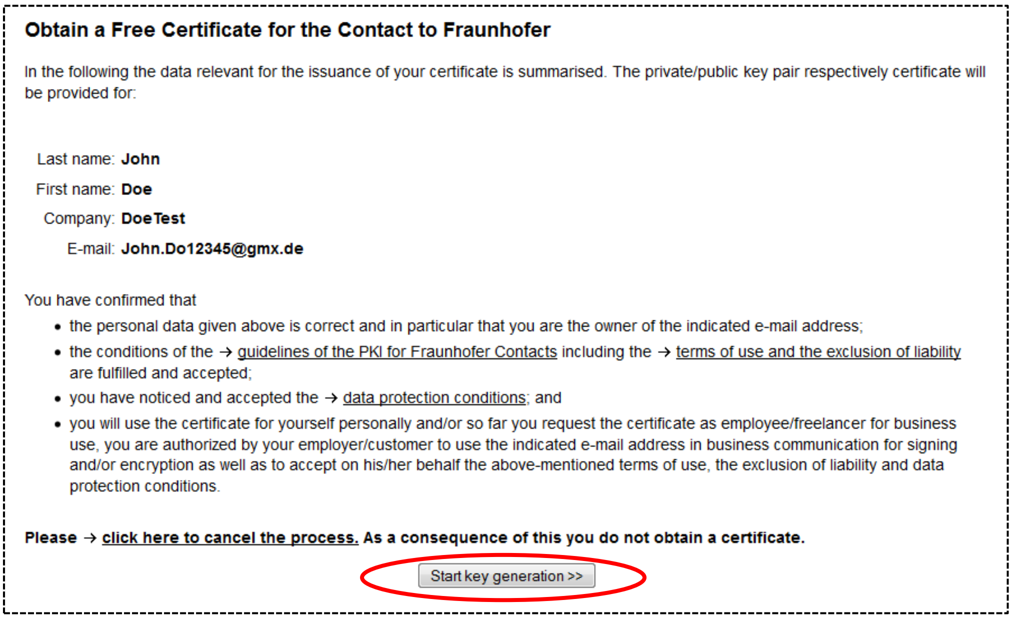
☑ **I confirm that I have noticed and accepted the → data protection conditions.**

☑ **I will use the certificate for myself personally and/or so far as I request the certificate as employee/freelancer for business use, I am authorized by my employer/customer to use the indicated e-mail address in business communication for signing and/or encryption as well as to accept on his/her behalf the above-mentioned terms of use, the exclusion of liability and data protection conditions.**

Figure 10: Certificate issuance with Mozilla Firefox – user's data check and confirmation of having read the guidelines for issuing certificates etc.

Now please check your personal information and confirm that it is correct. Please also confirm that you acknowledge and comply with the remaining specified conditions and disclaimers, in particular confirming that you have understood and will comply with the guidelines for the issuance of certificates of the PKI for Fraunhofer Contacts.

Click **Proceed to key generation** to be presented with a summary of the information you have entered and the confirmations you have given (see Figure 11). You also have the option to cancel the certificate generating process at this stage. Doing so means you will not receive a certificate.



Obtain a Free Certificate for the Contact to Fraunhofer

In the following the data relevant for the issuance of your certificate is summarised. The private/public key pair respectively certificate will be provided for:

Last name: **John**
First name: **Doe**
Company: **DoeTest**
E-mail: **John.Do12345@gmx.de**

You have confirmed that

- the personal data given above is correct and in particular that you are the owner of the indicated e-mail address;
- the conditions of the → guidelines of the PKI for Fraunhofer Contacts including the → terms of use and the exclusion of liability are fulfilled and accepted;
- you have noticed and accepted the → data protection conditions; and
- you will use the certificate for yourself personally and/or so far you request the certificate as employee/freelancer for business use, you are authorized by your employer/customer to use the indicated e-mail address in business communication for signing and/or encryption as well as to accept on his/her behalf the above-mentioned terms of use, the exclusion of liability and data protection conditions.

Please → click here to cancel the process. As a consequence of this you do not obtain a certificate.

Figure 11: Issuing certificates with Mozilla Firefox – summary of information entered by the user and the confirmations they have given

Click on **Start key generation** to generate a cryptographic key pair in your browser and to transmit the public key to the web server that will use it to create your certificate.

If your computer has a smartcard reader attached with a card inserted in it, you must select where you wish to save the key pair/certificate by choosing a token from the drop-down list in the token dialog box (see Figure 12). Select **Software Security Device** and confirm by clicking **OK**.

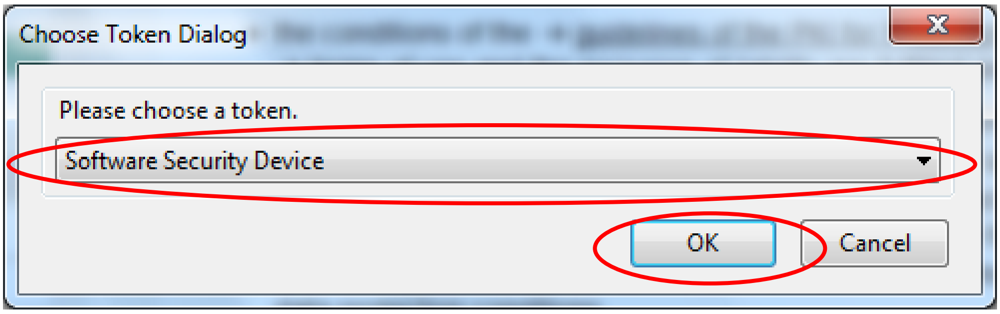
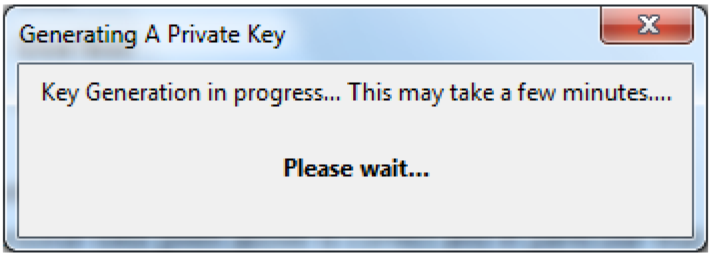


Figure 12: Issuing certificates with Mozilla Firefox – selecting where to save the key pair/certificate

Note: If your computer does not have a smartcard reader attached, or the smartcard reader contains the wrong card, the dialog window referred to above will not appear.

Note: If you have set your browser to require entry of a master password, you will now be asked to enter this password in order to access your software security module. The password is required because your personal certificate will be saved in the browser's certificate store.

You will then receive a message informing you that your key is being generated (see Figure 13).



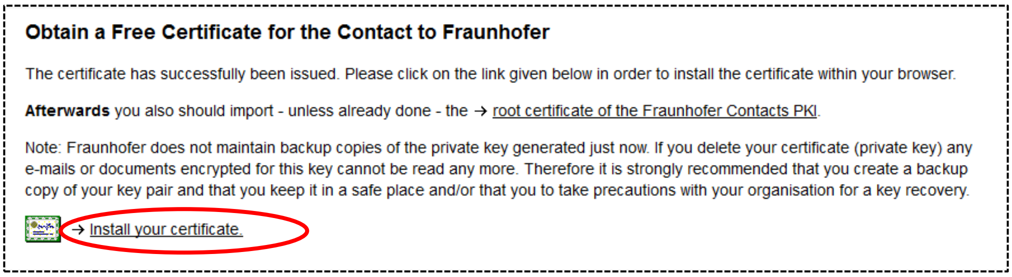
Generating A Private Key

Key Generation in progress... This may take a few minutes....

Please wait...

Figure 13: Certificate issuance with Mozilla Firefox – Generating the key pair

Once the keys have been generated and the certificate issued successfully, you will receive a message informing you that you can now install the certificate. Click on the **Install your certificate** link (see Figure 14). This process installs the certificate in the Firefox certificate store.



Obtain a Free Certificate for the Contact to Fraunhofer

The certificate has successfully been issued. Please click on the link given below in order to install the certificate within your browser.

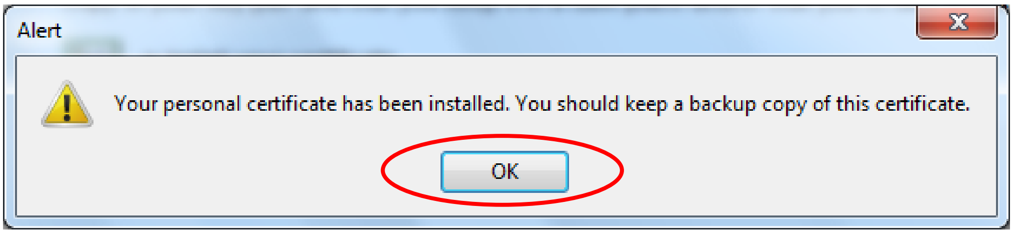
Afterwards you also should import - unless already done - the → root certificate of the Fraunhofer Contacts PKI.

Note: Fraunhofer does not maintain backup copies of the private key generated just now. If you delete your certificate (private key) any e-mails or documents encrypted for this key cannot be read any more. Therefore it is strongly recommended that you create a backup copy of your key pair and that you keep it in a safe place and/or that you to take precautions with your organisation for a key recovery.

→ Install your certificate.

Figure 14: Certificate issuance with Mozilla Firefox – Confirmation that the certificate was issued successfully

Mozilla Firefox generates a separate window to notify you that installation of the certificate was successful (see Figure 15). The system will issue an explicit reminder suggesting that you save a backup copy of the certificate. Confirm this suggestion with **OK**.



Your personal certificate has been installed. You should keep a backup copy of this certificate.

Figure 15: Certificate issuance with Mozilla Firefox – Confirmation that the certificate was installed successfully

Before the certificate can be used in your e-mail client, it must first be exported out of the browser and into your e-mail client. This process varies depending on the type of browser or e-mail client you use. How to export certificates from Mozilla Firefox is described in Section 3.2. How to use personal certificates in different e-mail clients is described in Chapter 0.

3 Exporting your own personal certificate from the browser

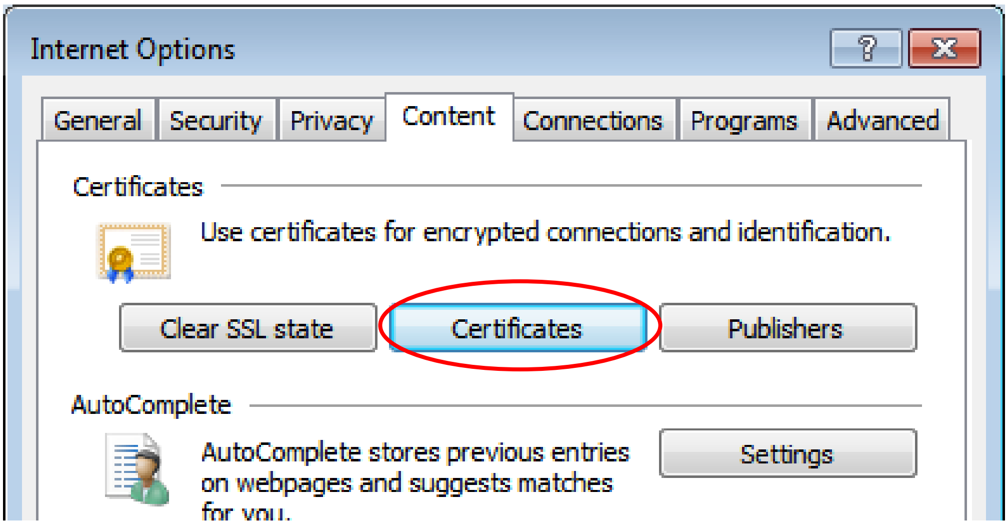
This chapter describes how to export personal certificates out of the browser.

Exporting certificates and the keys that go with them is necessary in order to be able to create local backup copies of the certificates. Furthermore, some combinations of browser and e-mail client require certificates (and private keys) to be integrated into the respective e-mail client manually. The following sections deal with the specifics of various possible combinations.

3.1 Exporting your own personal certificate from Microsoft Internet Explorer

Note: If you use Internet Explorer in combination with Microsoft Outlook or any other e-mail program that accesses the Microsoft certificate store, then it is not necessary to export personal certificates/keys to enjoy secure e-mail communication. Users are however still recommended to make a backup copy of the certificate (and private key).

Open the Microsoft certificate store in Internet Explorer by going to **Extras → Internet Options → Content → Certificates** (see Figure 16).

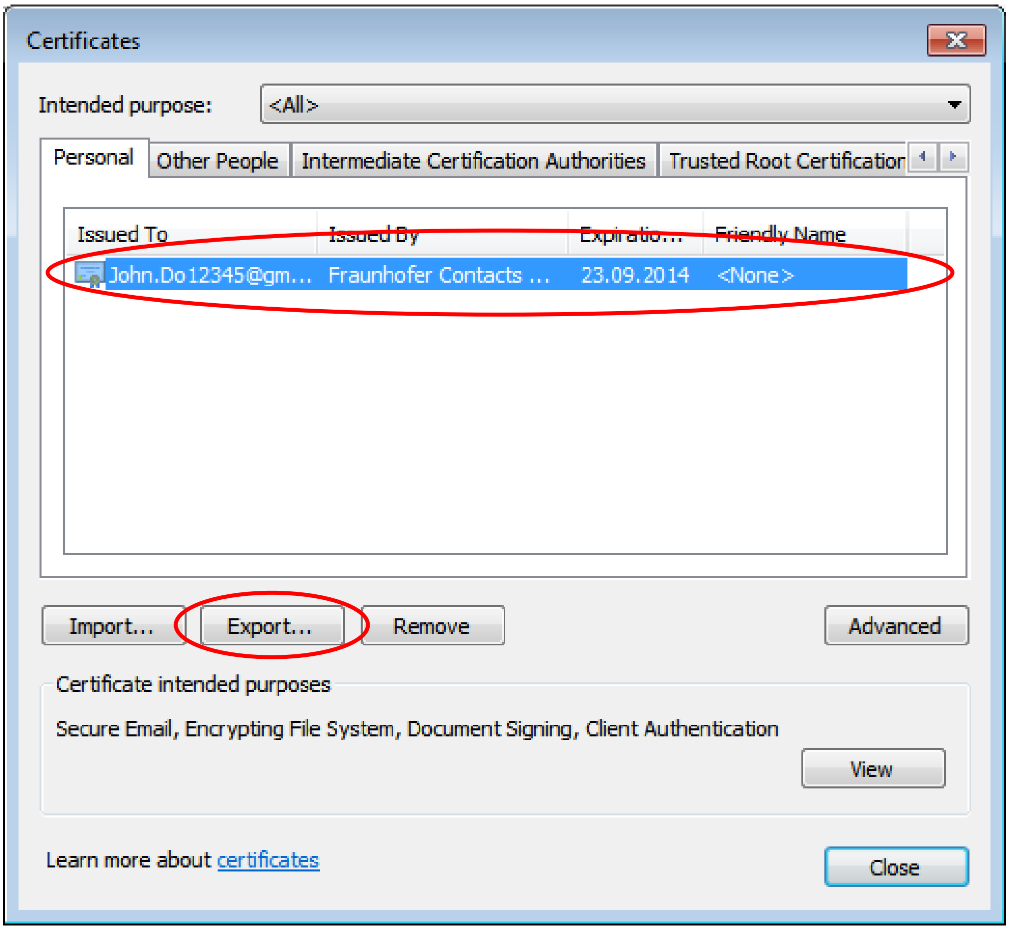


Use certificates for encrypted connections and identification.

AutoComplete stores previous entries on webpages and suggests matches for you.

Figure 16: Opening the Microsoft certificate store in Microsoft Internet Explorer

Select the certificate you wish to export from the options listed under the **Personal** tab and click **Export** (see Figure 17).



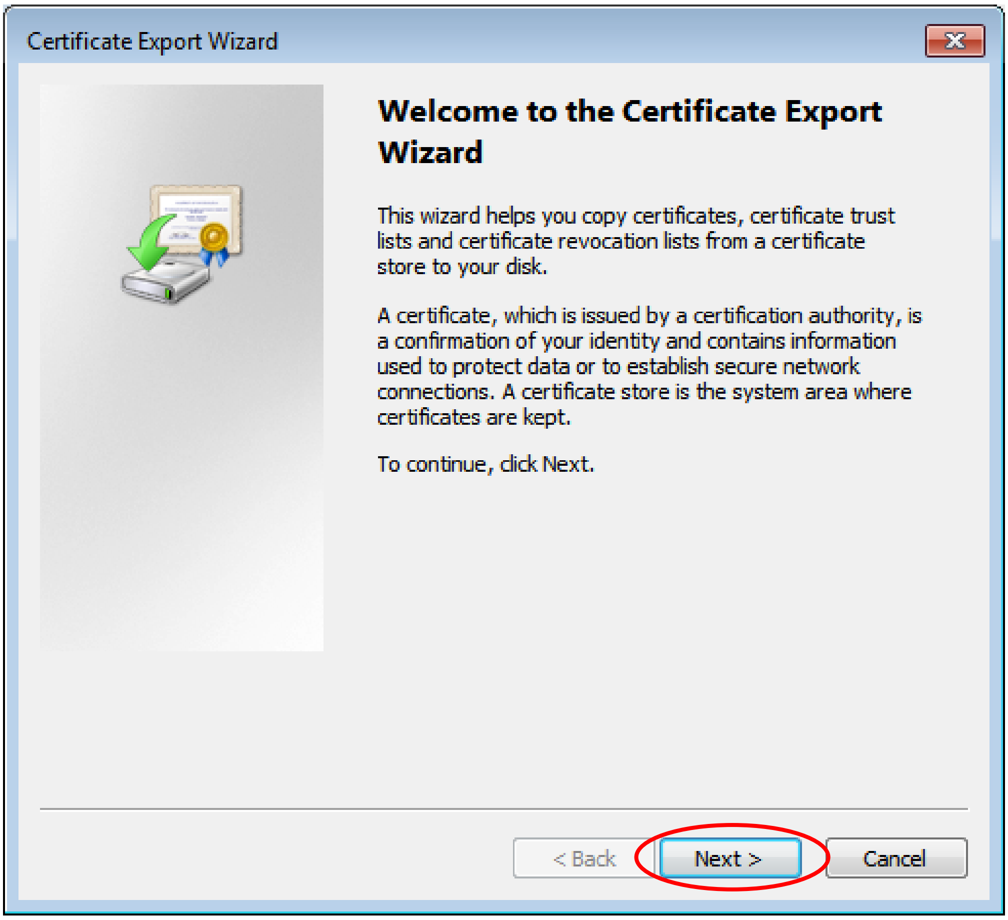
Issued To	Issued By	Expiratio...	Friendly Name
John.Do12345@gm...	Fraunhofer Contacts ...	23.09.2014	<None>

Certificate intended purposes

Secure Email, Encrypting File System, Document Signing, Client Authentication

Figure 17: Selecting the certificate that is to be exported from the Microsoft certificate store

This opens the Microsoft certificate export wizard, which will take you through the exporting process. Click **Next** (see Figure 18).



Welcome to the Certificate Export Wizard

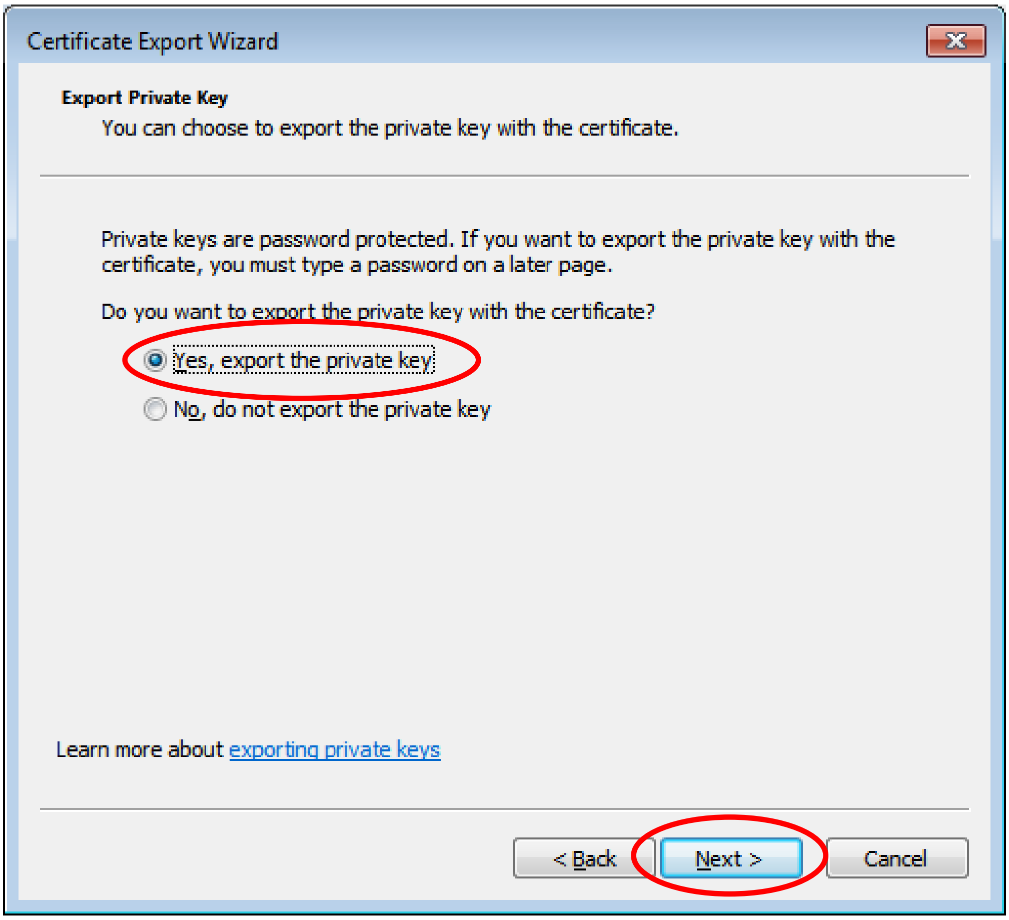
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

Figure 18: Microsoft certificate export wizard

Select the option **Yes, export the private key** in the dialog window that follows and confirm by clicking **Next** (see Figure 19).



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

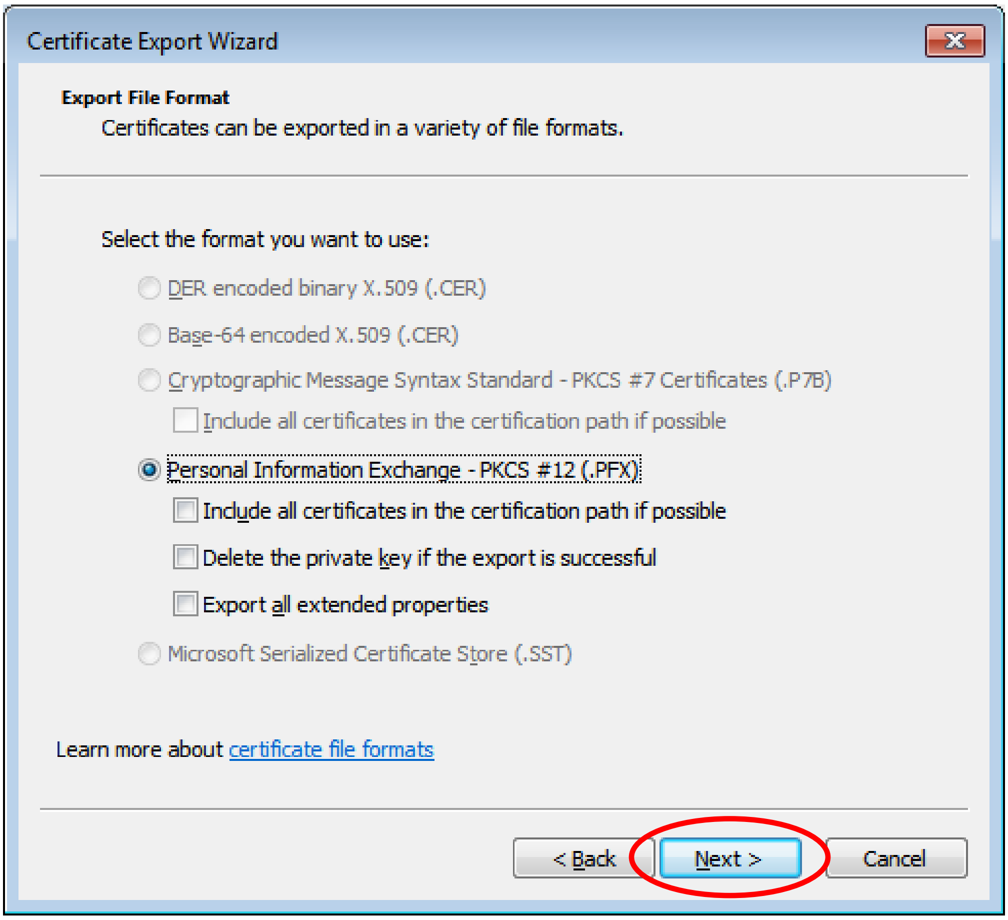
● Yes, export the private key

○ No, do not export the private key

Learn more about exporting private keys

Figure 19: Microsoft certificate export wizard – Selecting the option for exporting the private key

You do not need to make any changes in the dialog windows that follow, and can simply click **Next** (see Figure 20).



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

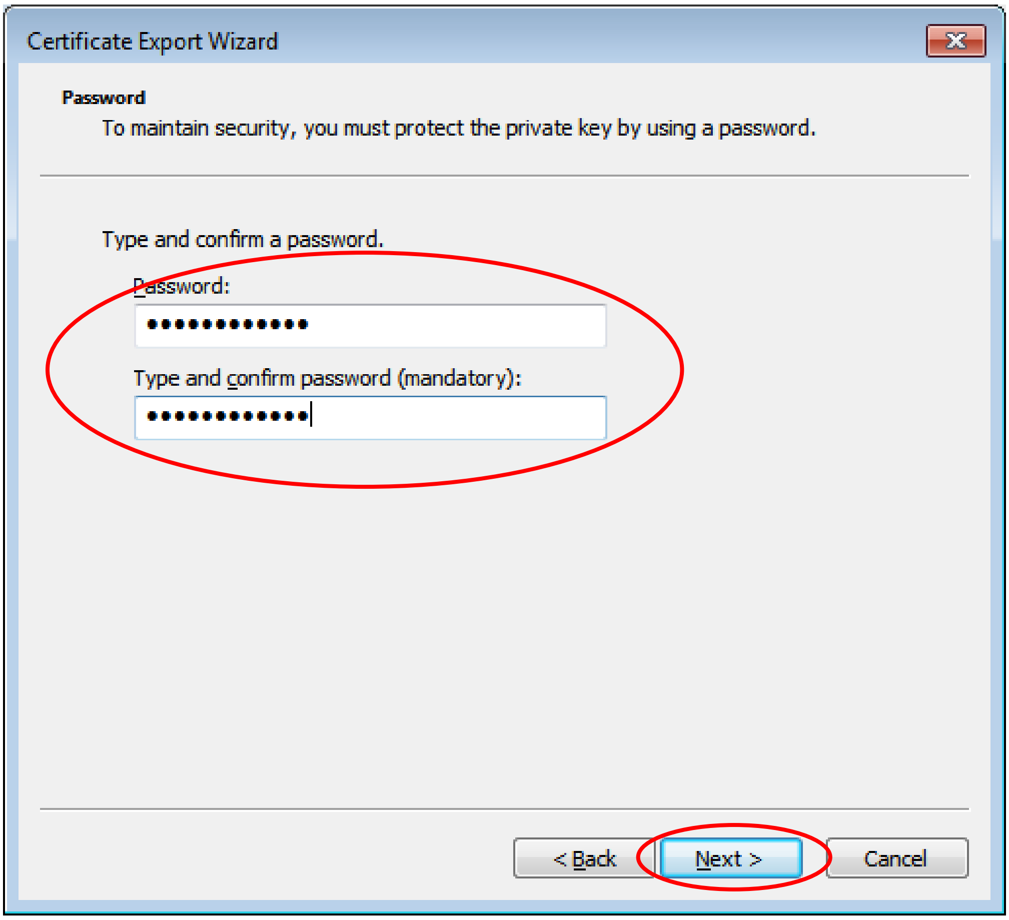
○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Figure 20: Microsoft certificate cxport wizard – Selecting the file export format

Now enter a secure password[1] to protect the key when it is exported (see Figure 21). The password will be required whenever you want to import your certificate into a program, and protects against unauthorized access. Confirm this dialog window by clicking **Next**.

[1] The password should be at least twelve characters long and contain upper and lower case letters, numbers and symbols.



Certificate Export Wizard

Password

To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password: ●●●●●●●●●●●●

Type and confirm password (mandatory): ●●●●●●●●●●●●

Figure 21: Microsoft certificate export wizard – Entering the transport password for the backup certificate

Now click on **Browse** and select a location in which to save the certificate. Give the certificate and key file names that aptly describe the content, click **Save** and confirm the remaining dialog by clicking **Next** (see Figure 22).

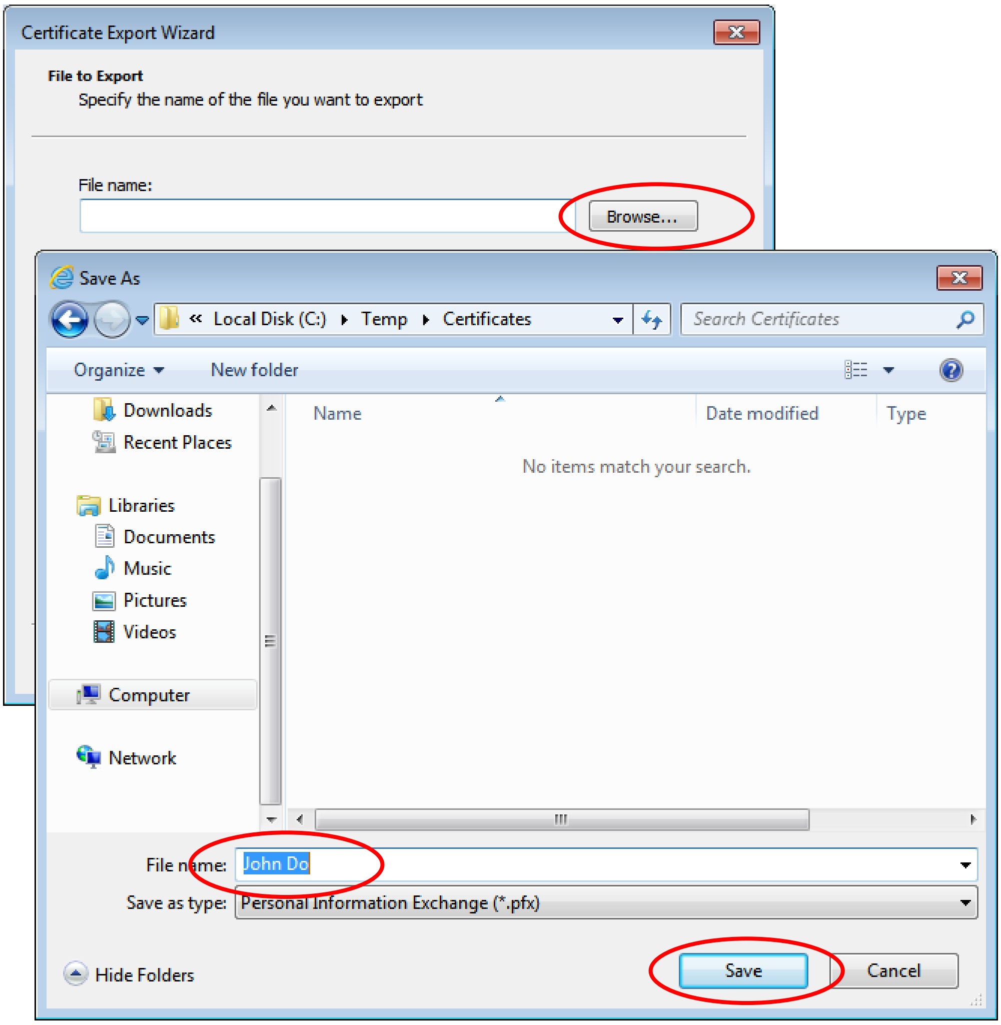
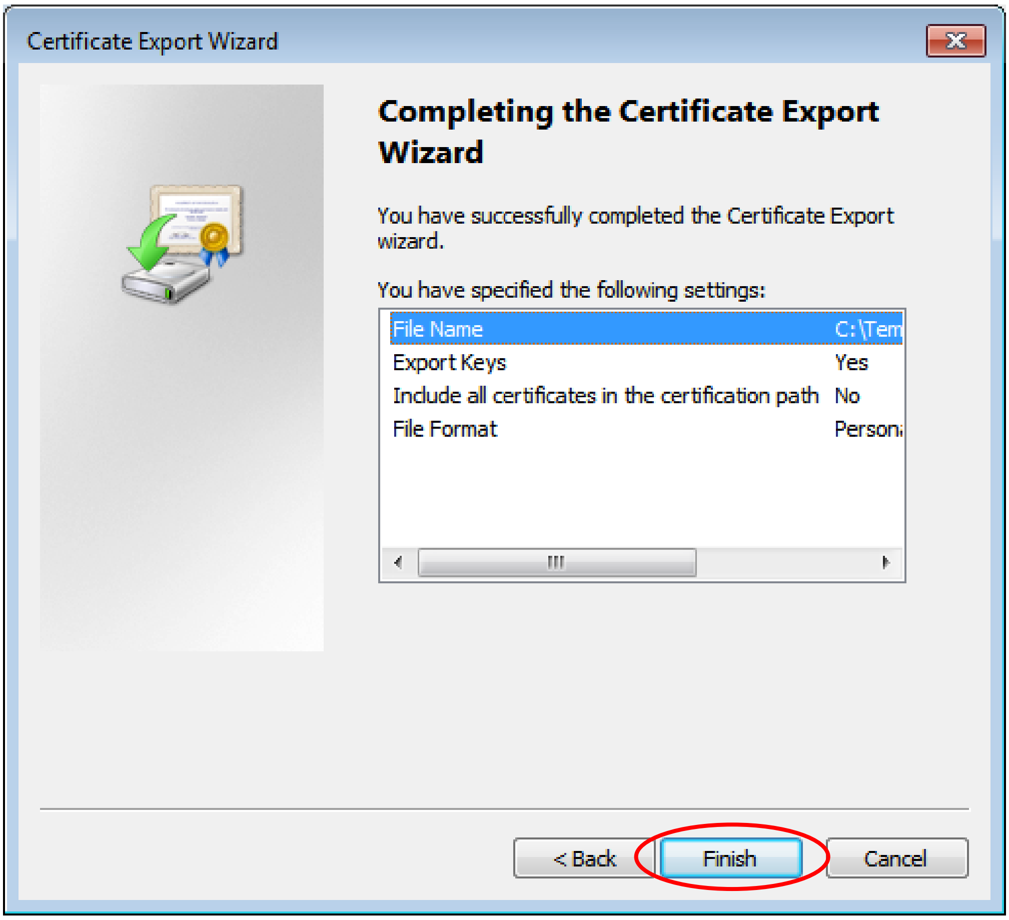


Figure 22: Microsoft certificate export wizard – Selecting where to save the backup certificate

The Certificate Export Wizard now presents you with another summary of the settings you have chosen. Click on **Finish** to execute and complete the export process (see Figure 23).



Certificate Export Wizard

Completing the Certificate Export Wizard

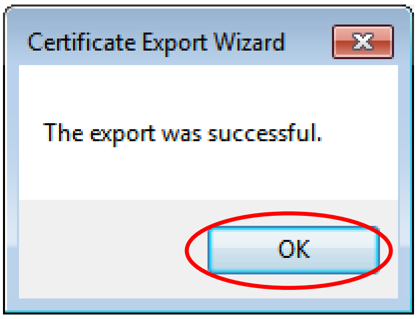
You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Tem
Export Keys	Yes
Include all certificates in the certification path	No
File Format	Person

Figure 23: Microsoft certificate export wizard – Finishing the wizard

A message will appear to confirm that the export was carried out successfully. Confirm it by clicking **OK** (see Figure 24).



Certificate Export Wizard

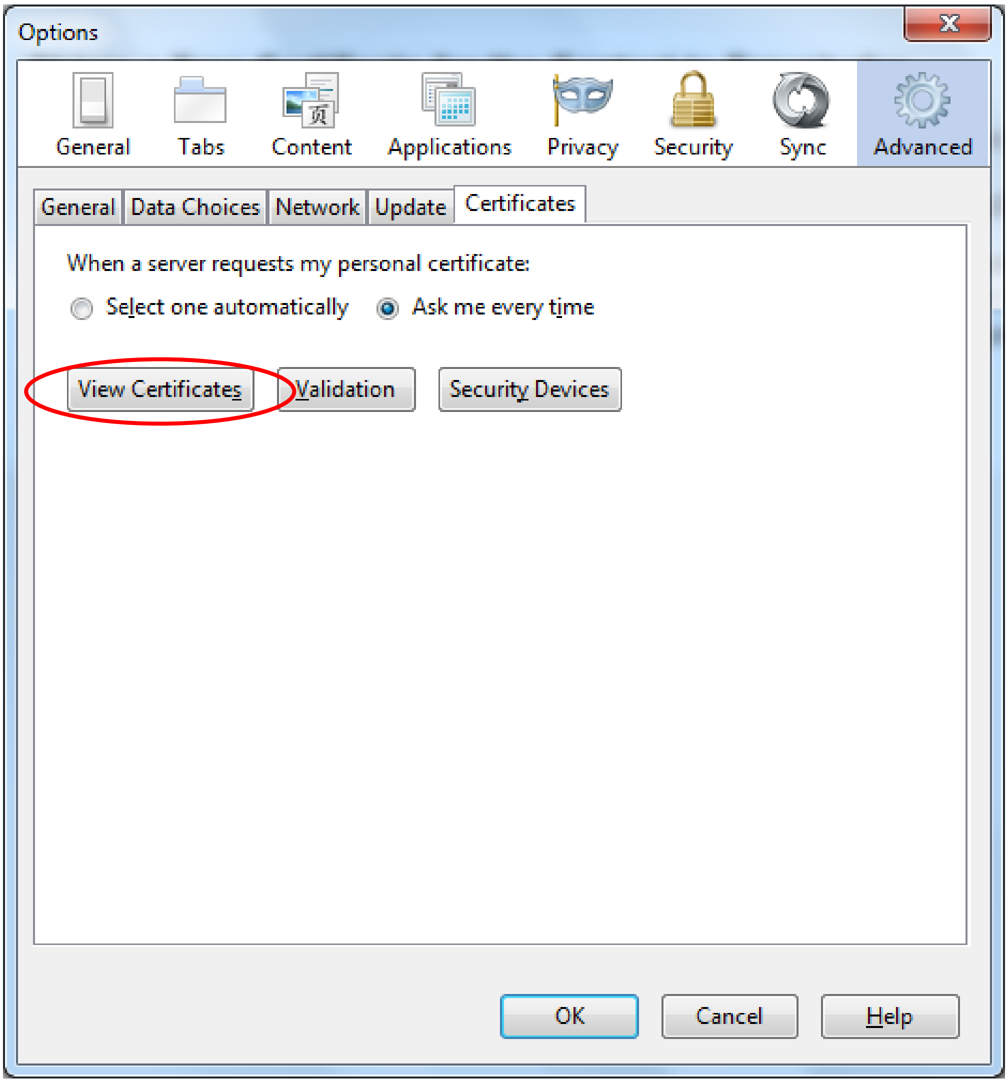
The export was successful.

Figure 24: Microsoft certificate export wizard – Message informing you that certificate and private key were successfully exported

3.2 Exporting your own personal certificate from Mozilla Firefox

Note: Regardless of the e-mail program you use in combination with Mozilla Firefox, secure e-mail communication is possible only if personal certificates/keys are first exported out of the browser (and imported into the respective e-mail program). The Mozilla Firefox certificate manager can be accessed only from within the browser itself. Beyond this it also makes sense to export the certificate and private key in order to back them up.

Open the Mozilla Firefox certificate manager via **Extras → Options → Advanced → Certificates → View Certificates** (see Figure 25).

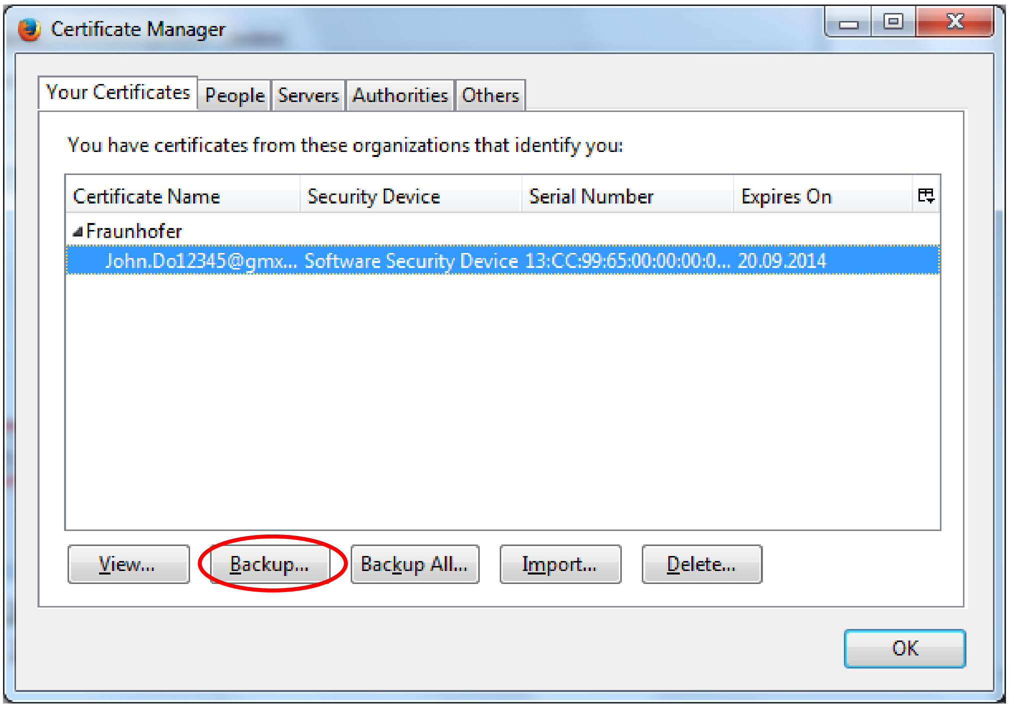


When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

Figure 25: Opening the Mozilla Firefox certificate manager

Next, select the certificate you wish to export from the options listed under the **Your Certificates** tab and click on **Backup** (see Figure 26).

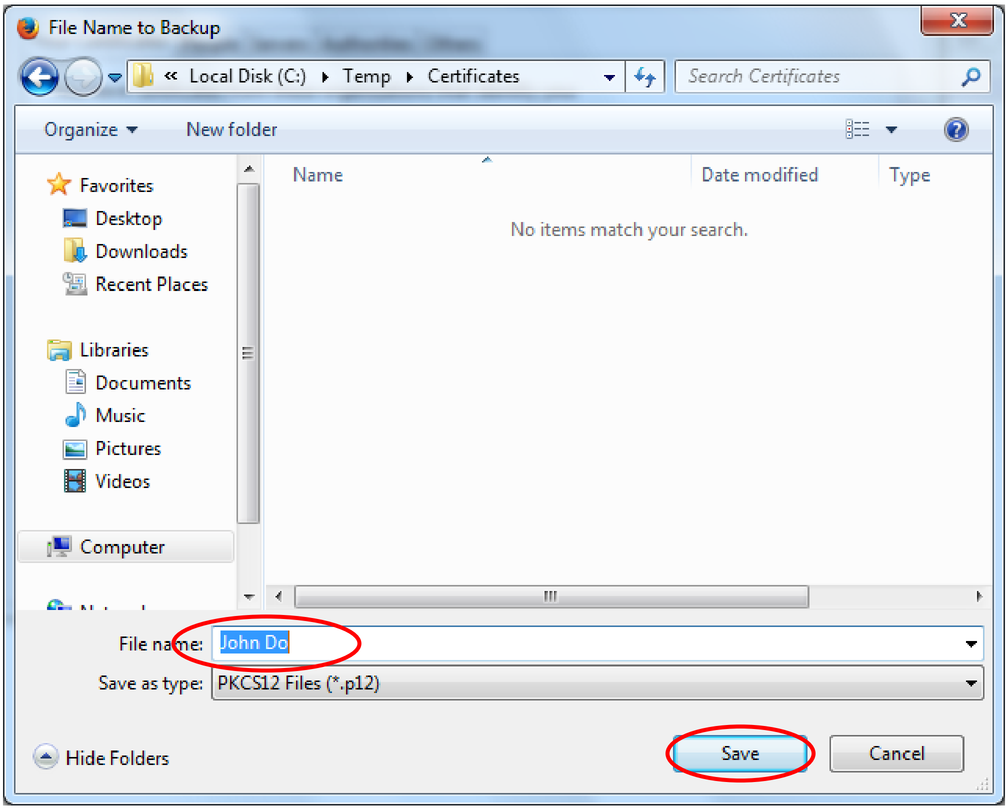


You have certificates from these organizations that identify you:

Certificate Name	Security Device	Serial Number	Expires On
Fraunhofer			
John.Do12345@gmx...	Software Security Device	13:CC:99:65:00:00:00:0...	20.09.2014

Figure 26: Selecting the certificate that is to be exported from the Mozilla Firefox certificate manager

Now select a location in which to save the certificate. Give the certificate and key file names that aptly describe the content, and then click **Save** (see Figure 27).



No items match your search.

File name: John Do

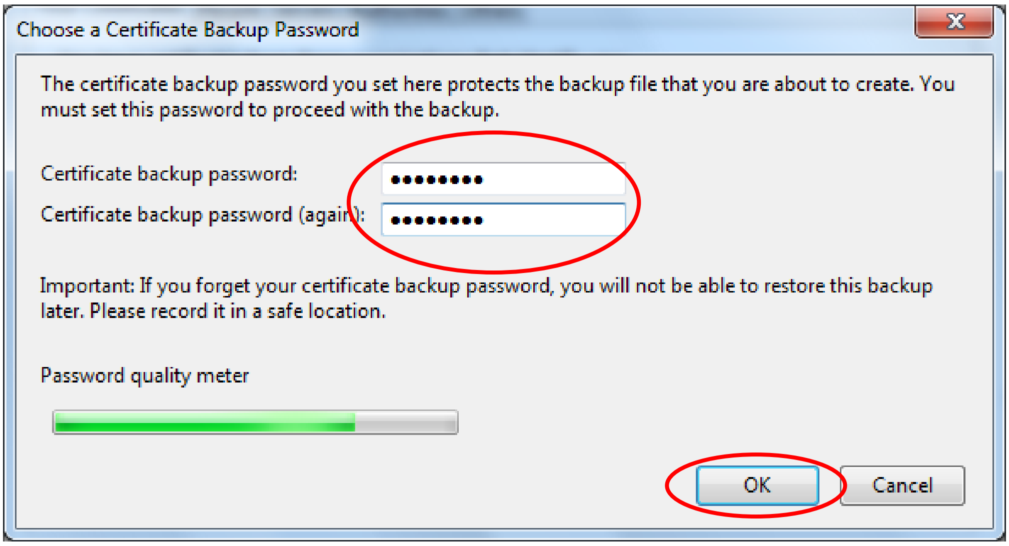
Save as type: PKCS12 Files (*.p12)

Figure 27: Selecting where to save the backup certificate in Mozilla Firefox

Note: If you have set your browser to require entry of a master password, you will now be asked to enter this password in order to access your software security module. The password is required because your personal certificate and the private key that goes with it will be exported out of the browser's certificate manager.

Now enter a secure password[2] to protect the key when it is exported (see Figure 28). The password will be required whenever you want to import your certificate into a program, and protects against unauthorized access. Confirm this dialog window by clicking **OK**.

[2] The password should be at least twelve characters long and contain upper and lower case letters, numbers and symbols.



Choose a Certificate Backup Password

The certificate backup password you set here protects the backup file that you are about to create. You must set this password to proceed with the backup.

Certificate backup password: ••••••••

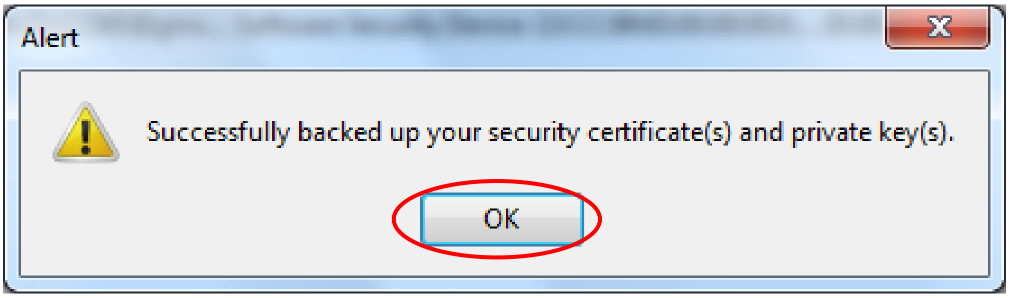
Certificate backup password (again): ••••••••

Important: If you forget your certificate backup password, you will not be able to restore this backup later. Please record it in a safe location.

Password quality meter

Figure 28: Entering the transport password for the backup certificate (Mozilla Firefox)

A message will appear to confirm that the backup process was carried out successfully. Confirm by clicking **OK** (see Figure 29).



Alert

Successfully backed up your security certificate(s) and private key(s).

Figure 29: Message informing you that certificate and private key were successfully backed up (Mozilla Firefox)

4 Using certificates within an e-mail client

This section describes how to use your own personal certificate to communicate securely with a Fraunhofer employee. To do you will first have to integrate both the root certificate of the PKI for Fraunhofer Contacts and your own certificate into your e-mail client/application.

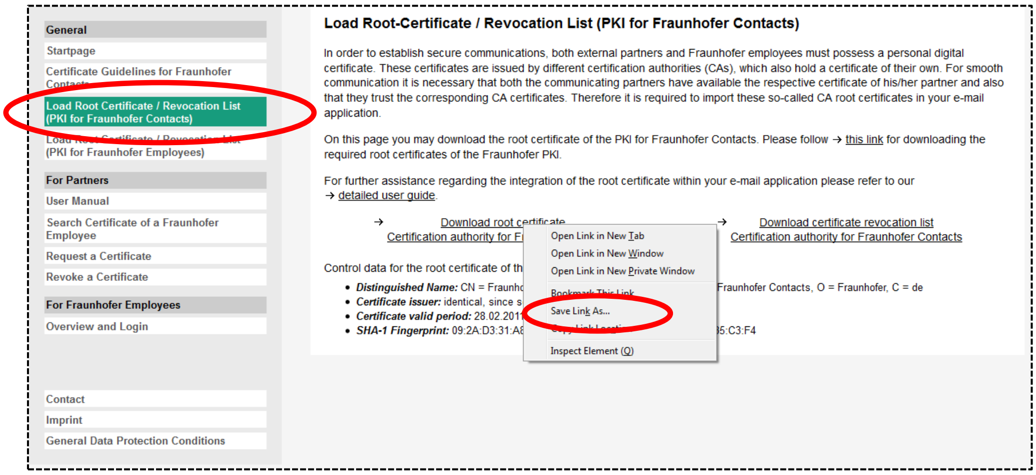
A further requirement for setting up encrypted communication with a Fraunhofer employee is that you integrate their encryption certificate in your e-mail client. In exceptional cases it may also be necessary to integrate the root certificate, that is to say the PKI for Fraunhofer Employees certificate chain, into the e-mail client as well. Instructions on how to proceed in such instances are also included in this section.

4.1 Preparing the e-mail client to use certificates

Different e-mail clients have to be prepared in different ways, so you must follow the instructions applicable to the kind of e-mail client you use. This section describes the process for applications that access the Microsoft certificate store (such as Microsoft Outlook) as well as for applications that use their own certificate store (such as Mozilla Thunderbird).

4.1.1 Integrating the PKI for Fraunhofer Contacts root certificate

First download the root certificate from the website at https://contacts.pki.fraunhofer.de. Do so by clicking **Load Root Certificate / Revocation List (PKI for Fraunhofer Contacts)** under the **General** menu heading. This opens another page. Right-click on the **Download root certificate Certification authority for Fraunhofer Contacts** link and select **Save Link As** from the context menu that appears (see **Figure 30**).


General
Startpage
Certificate Guidelines for Fraunhofer Contacts
Load Root Certificate / Revocation List (PKI for Fraunhofer Contacts)
Load Root Certificate / Revocation List (PKI for Fraunhofer Employees)
For Partners
User Manual
Search Certificate of a Fraunhofer Employee
Request a Certificate
Revoke a Certificate
For Fraunhofer Employees
Overview and Login
Contact
Imprint
General Data Protection Conditions
Open Link in New Tab
Open Link in New Window
Open Link in New Private Window
Bookmark This Link
Save Link As...
Copy Link Location
Inspect Element (Q)

Load Root-Certificate / Revocation List (PKI for Fraunhofer Contacts)

In order to establish secure communications, both external partners and Fraunhofer employees must possess a personal digital certificate. These certificates are issued by different certification authorities (CAs), which also hold a certificate of their own. For smooth communication it is necessary that both the communicating partners have available the respective certificate of his/her partner and also that they trust the corresponding CA certificates. Therefore it is required to import these so-called CA root certificates in your e-mail application.

On this page you may download the root certificate of the PKI for Fraunhofer Contacts. Please follow → this link for downloading the required root certificates of the Fraunhofer PKI.

For further assistance regarding the integration of the root certificate within your e-mail application please refer to our → detailed user guide.

→ Download root certificate
Certification authority for Fr

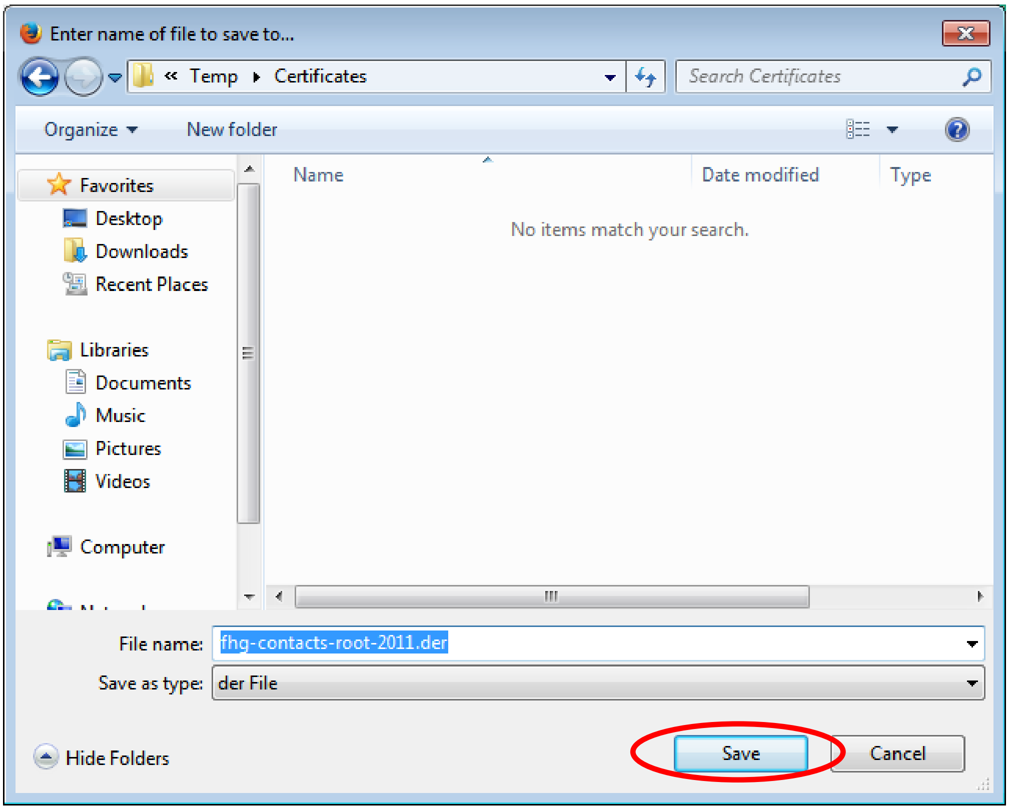
→ Download certificate revocation list
Certification authority for Fraunhofer Contacts

Control data for the root certificate of th

- ***Distinguished Name:*** CN = Fraunho Fraunhofer Contacts, O = Fraunhofer, C = de
- ***Certificate issuer:*** identical, since s
- ***Certificate valid period:*** 28.02.201
- ***SHA-1 Fingerprint:*** 09:2A:D3:31:A8 5:C3:F4

Figure 30: Downloading the PKI for Fraunhofer Contacts root certificate

Now select the file where you wish to save the certificate, and click **Save** (see **Figure 31**).



File name: fhg-contacts-root-2011.der

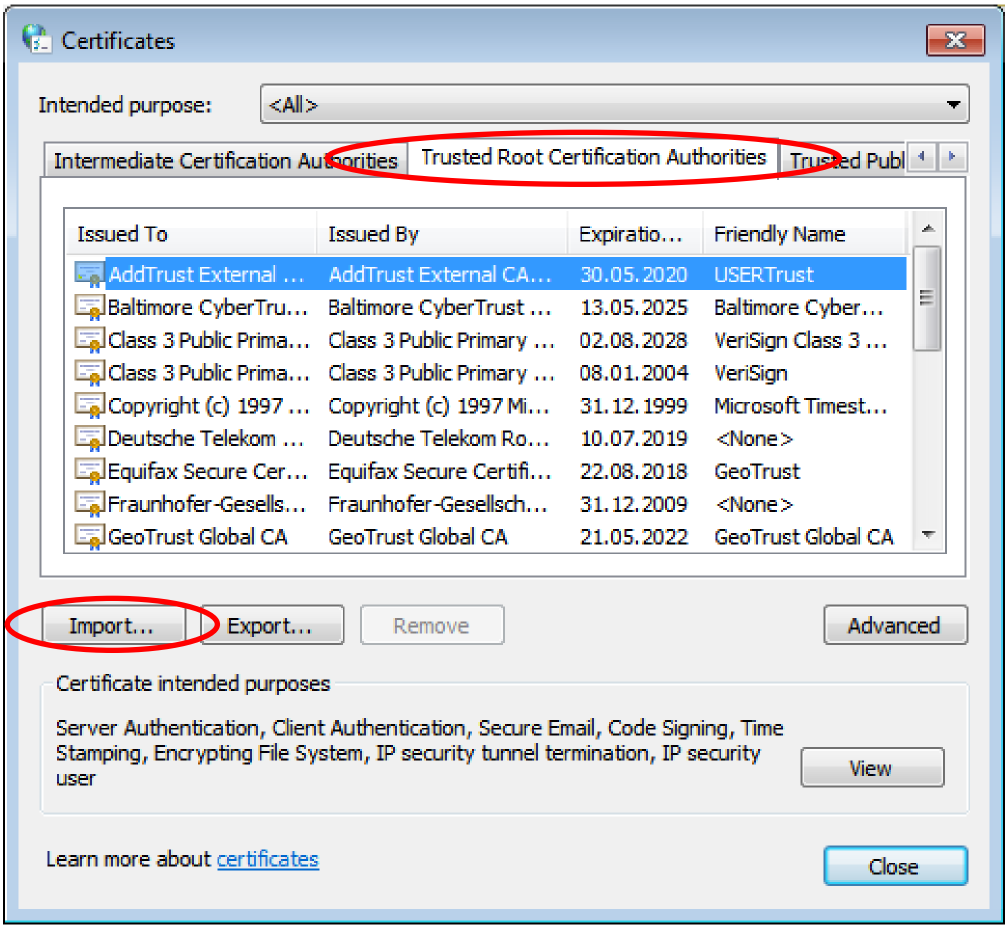
Save as type: der File

Figure 31: Saving the PKI for Fraunhofer Contacts root certificate

4.1.1.1 Incorporating the PKI for Fraunhofer Contacts root certificate into the Microsoft certificate store

If you use Microsoft Outlook for your e-mail communication, then the PKI for Fraunhofer Contacts root certificate must be imported into the Microsoft certificate store that Microsoft Outlook also accesses.

To do so, open the Microsoft certificate store via **Start →Control panel → Network and Internet → Internet options → Content → Certificates** and open up the **Trusted Root Certification Authorities** tab. Click on **Import** (see **Figure 32**).



Issued To	Issued By	Expiratio...	Friendly Name
AddTrust External ...	AddTrust External CA...	30.05.2020	USERTrust
Baltimore CyberTru...	Baltimore CyberTrust ...	13.05.2025	Baltimore Cyber...
Class 3 Public Prima...	Class 3 Public Primary ...	02.08.2028	VeriSign Class 3 ...
Class 3 Public Prima...	Class 3 Public Primary ...	08.01.2004	VeriSign
Copyright (c) 1997 ...	Copyright (c) 1997 Mi...	31.12.1999	Microsoft Timest...
Deutsche Telekom ...	Deutsche Telekom Ro...	10.07.2019	<None>
Equifax Secure Cer...	Equifax Secure Certifi...	22.08.2018	GeoTrust
Fraunhofer-Gesells...	Fraunhofer-Gesellsch...	31.12.2009	<None>
GeoTrust Global CA	GeoTrust Global CA	21.05.2022	GeoTrust Global CA

Certificate intended purposes

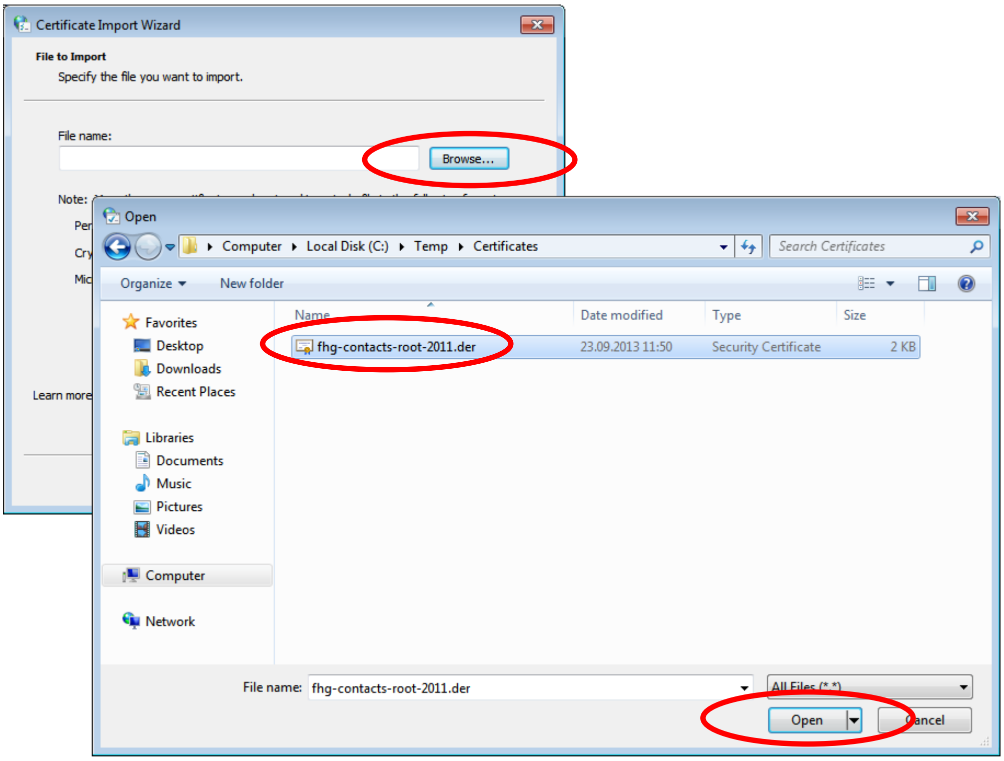
Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping, Encrypting File System, IP security tunnel termination, IP security user

Learn more about certificates

Figure 32: Screenshot showing the Microsoft certificate store's *Trusted Root Certification Authorities*

This opens the certificate import wizard. Confirm the first window by clicking **Next**. Now click the **Browse...** button and select the root certificate that was downloaded previously. Confirm the dialog window by clicking **Open** and then on **Next** (see **Figure 33**).

Note: If the PKI for Fraunhofer Contacts root certificate is not shown in the 'Open' dialog window, you must change the filter that determines the file types shown from "X.509 Certificate (*.cer,*.crt)" to "All Files (*.*)", the option that shows all types of file.



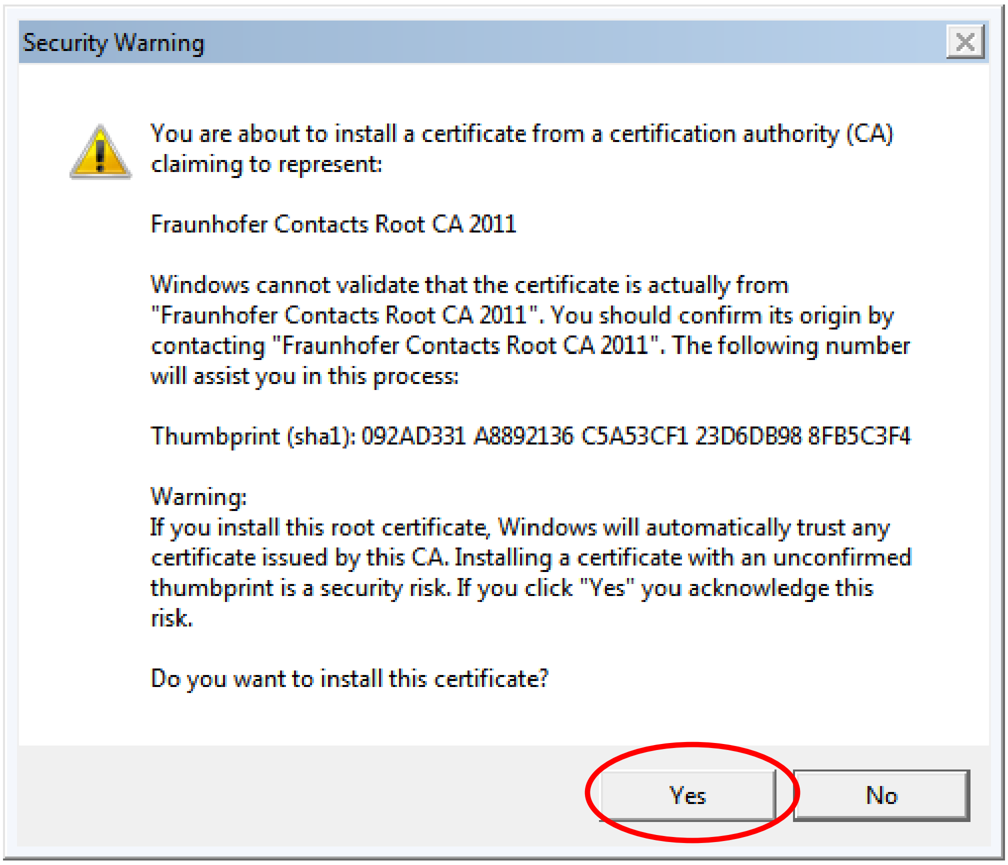
Name	Date modified	Type	Size
fhg-contacts-root-2011.der	23.09.2013 11:50	Security Certificate	2 KB

File name: fhg-contacts-root-2011.der

All Files (*.*)

Figure 33: Selecting the PKI for Fraunhofer Contacts root certificate when importing it into the Microsoft certificate store

In the dialog windows that follow, simply assume the standard settings and confirm them by clicking **Next**. Finish the certificate import wizard by clicking **Finish**. At the end of the installation process you will be presented with a security warning (see **Figure 34**). After you have verified that the fingerprint cited in the security dialog box is correct, please confirm by clicking **Yes**. Verify the fingerprint by carefully comparing the fingerprint shown in the security dialog box with the root certificate fingerprint given on the website. Confirm by clicking **Yes** only if all the characters (letters and digits) in both keys are absolutely identical.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

Fraunhofer Contacts Root CA 2011

Windows cannot validate that the certificate is actually from "Fraunhofer Contacts Root CA 2011". You should confirm its origin by contacting "Fraunhofer Contacts Root CA 2011". The following number will assist you in this process:

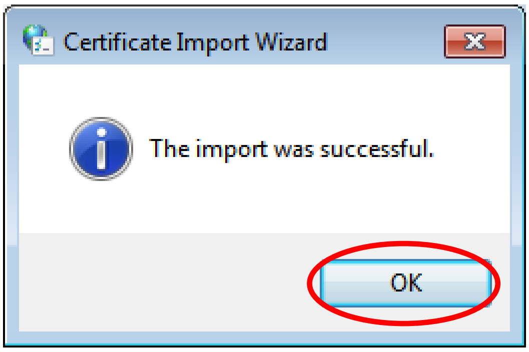
Thumbprint (sha1): 092AD331 A8892136 C5A53CF1 23D6DB98 8FB5C3F4

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Figure 34: Security warning when importing the PKI for Fraunhofer Contacts root certificate into the Microsoft certificate store

A message will appear to confirm that the import was carried out successfully. Close the window by clicking **OK** (see **Figure 35**).



Certificate Import Wizard

The import was successful.

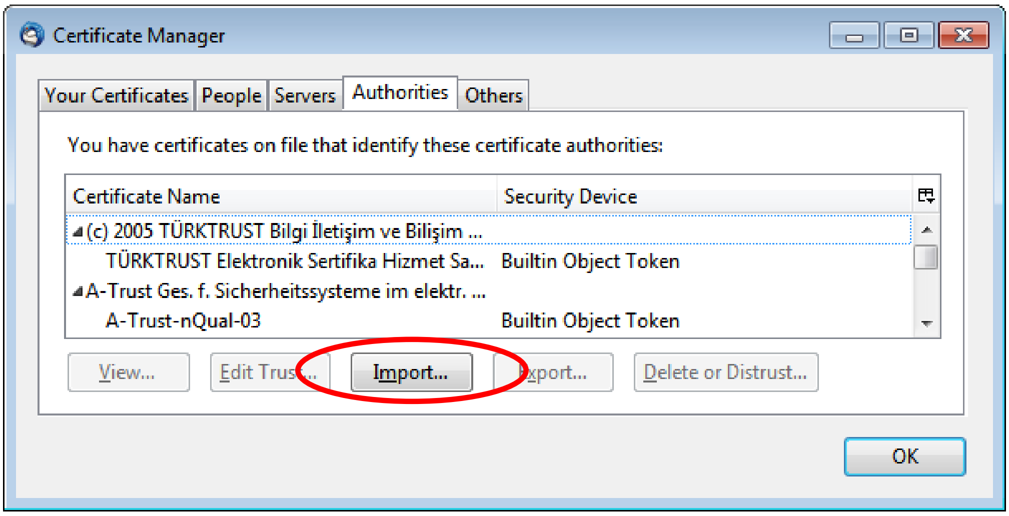
Figure 35: Importing the PKI for Fraunhofer Contacts root certificate into the Microsoft certificate store was successful

4.1.1.2 Incorporating the PKI for Fraunhofer Contacts root certificate into the Mozilla Thunderbird certificate manager

If you use Mozilla Thunderbird for your e-mail communication, then the PKI for Fraunhofer Contacts root certificate must be imported into the Mozilla Thunderbird certificate manager.

Note: Mozilla Firefox and Mozilla Thunderbird each use their own certificate managers.

To import the root certificate into the Thunderbird certificate manager, open the certificate manager via **Extras → Options → Advanced → Certificates → View Certificates** and open up the **Authorities** tab. Click on **Import** (see **Figure 36**).

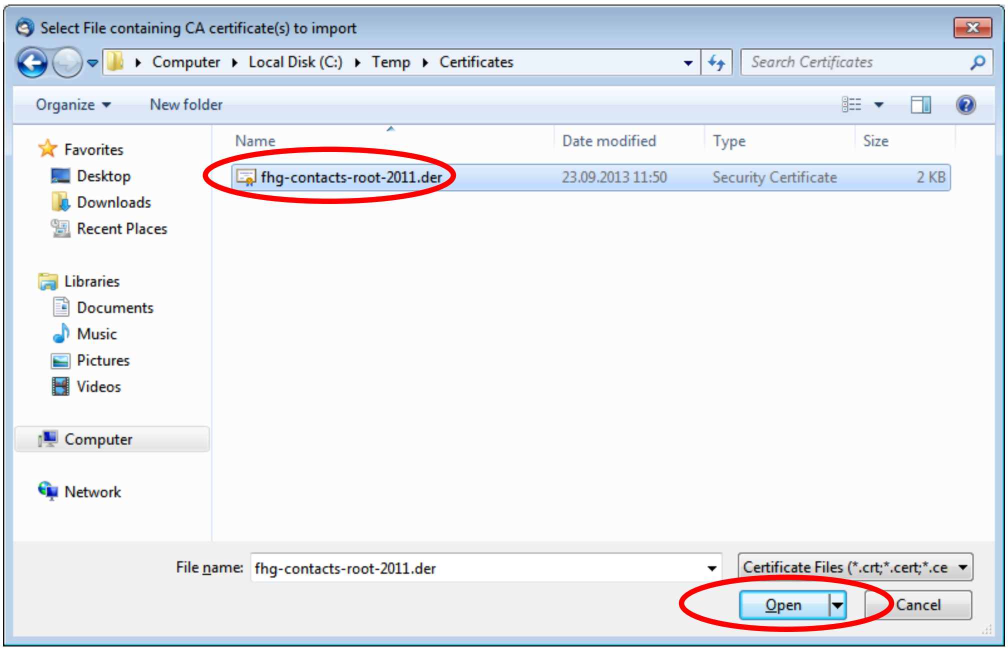


You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
◢(c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim ...	
TÜRKTRUST Elektronik Sertifika Hizmet Sa...	Builtin Object Token
◢A-Trust Ges. f. Sicherheitssysteme im elektr. ...	
A-Trust-nQual-03	Builtin Object Token

Figure 36: Screenshot showing the Thunderbird Certificate manager's *Certificate authorities*

This opens a file selection dialog window. Navigate to the location where you saved the PKI for Fraunhofer Contacts root certificate and select the root certificate that was downloaded previously. Confirm the dialog window by clicking **Open** (see **Figure 37**).



Select File containing CA certificate(s) to import

Computer ▸ Local Disk (C:) ▸ Temp ▸ Certificates

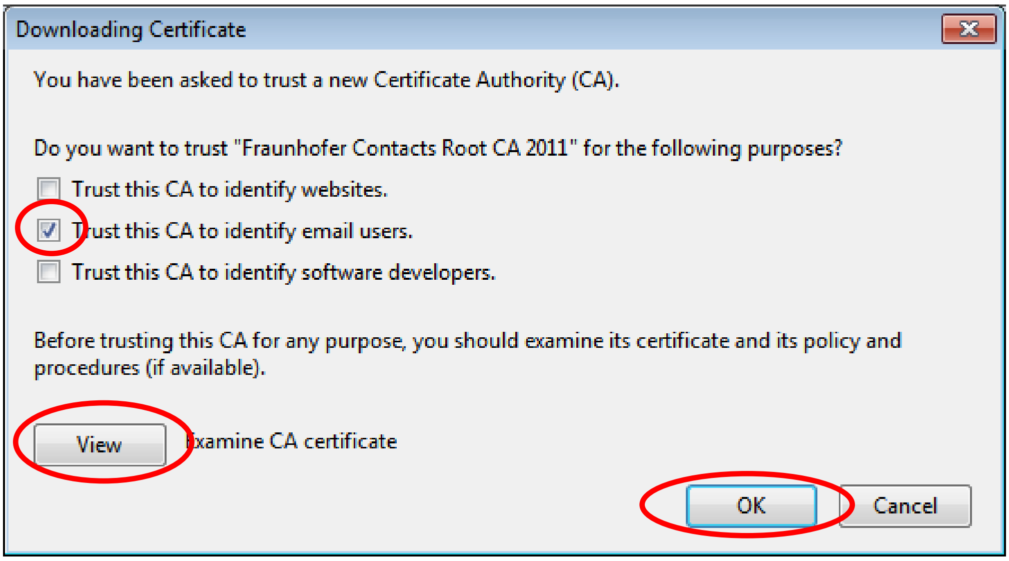
Name	Date modified	Type	Size
fhg-contacts-root-2011.der	23.09.2013 11:50	Security Certificate	2 KB

File name: fhg-contacts-root-2011.der

Certificate Files (*.crt;*.cert;*.ce

Figure 37: Selecting the PKI for Fraunhofer Contacts root certificate when importing it into the Thunderbird certificate manager

Now confirm the purpose for which you would like the certificate to be trusted. Ensure that at least the *Trust this CA to identify email users* option is selected, and close the dialog window by clicking **OK** after you have made sure that the certificate's SHA1 fingerprint precisely matches the root certificate fingerprint given on the website (see **Figure 38**). To see the fingerprint for the certificate that is to be imported, please click **View**. The SHA1 fingerprint is shown at the bottom of the **General** tab. All the characters (letters and digits) must be absolutely identical to the fingerprint key given on the website.



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "Fraunhofer Contacts Root CA 2011" for the following purposes?

□ Trust this CA to identify websites.

☑ Trust this CA to identify email users.

□ Trust this CA to identify software developers.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Figure 38: Selecting the trust settings for the PKI for Fraunhofer Contacts root certificate when importing it into Mozilla Thunderbird.

The PKI for Fraunhofer Contacts root certificate is now available in the certificate manager and can now be used by Mozilla Thunderbird to verify user certificates from the PKI for Fraunhofer Contacts.

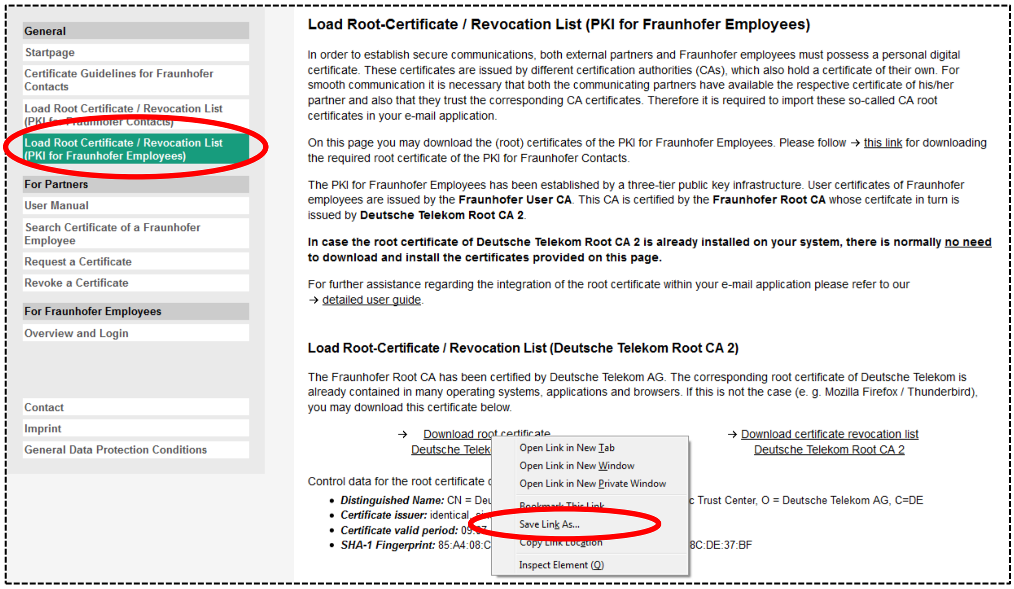
4.1.2 Integrating the PKI for Fraunhofer Employees root certificate / certificate chain

In order to be able to verify and use Fraunhofer employee certificates, you must also trust the certification authority that issued the employee certificates. Unlike the PKI for Fraunhofer Contacts, the Fraunhofer-Gesellschaft's PKI for its employees consists of a multi-level hierarchy that has the *Deutsche Telekom Root CA 2* certificate as root certificate at the very top.

Note: In the great majority of cases, the *Deutsche Telekom Root CA 2* root certificate is pre-installed as standard in operating systems, browsers and e-mail applications. This means a separate import process is not usually necessary. Perform the import only if you encounter problems when verifying or using Fraunhofer employee certificates. In some individual cases it may be necessary to import the remaining certificates in the Fraunhofer PKI certificate chain in addition to the *Deutsche Telekom Root CA 2* root certificate, these being the *Fraunhofer Root CA 2007* certificate and the *Fraunhofer User CA 2007* certificate.

You can download the PKI for Fraunhofer Employees root certificate and the remaining certificates of the corresponding certificate chain from the https://contacts.pki.fraunhofer.de page. Do so by clicking **Load Root Certificate /**

Revocation List (PKI for Fraunhofer Employees) under the **General** menu heading. This opens another page. Right-click on the **Download Root Certificate Deutsche Telekom Root CA 2** link and select **Save Link As** from the context menu that appears (see Figure 39).



General
Startpage
Certificate Guidelines for Fraunhofer Contacts
Load Root Certificate / Revocation List (PKI for Fraunhofer Contacts)
Load Root Certificate / Revocation List (PKI for Fraunhofer Employees)
For Partners
User Manual
Search Certificate of a Fraunhofer Employee
Request a Certificate
Revoke a Certificate
For Fraunhofer Employees
Overview and Login
Contact
Imprint
General Data Protection Conditions

Load Root-Certificate / Revocation List (PKI for Fraunhofer Employees)

In order to establish secure communications, both external partners and Fraunhofer employees must possess a personal digital certificate. These certificates are issued by different certification authorities (CAs), which also hold a certificate of their own. For smooth communication it is necessary that both the communicating partners have available the respective certificate of his/her partner and also that they trust the corresponding CA certificates. Therefore it is required to import these so-called CA root certificates in your e-mail application.

On this page you may download the (root) certificates of the PKI for Fraunhofer Employees. Please follow → this link for downloading the required root certificate of the PKI for Fraunhofer Contacts.

The PKI for Fraunhofer Employees has been established by a three-tier public key infrastructure. User certificates of Fraunhofer employees are issued by the **Fraunhofer User CA**. This CA is certified by the **Fraunhofer Root CA** whose certifcate in turn is issued by **Deutsche Telekom Root CA 2**.

In case the root certificate of Deutsche Telekom Root CA 2 is already installed on your system, there is normally no need to download and install the certificates provided on this page.

For further assistance regarding the integration of the root certificate within your e-mail application please refer to our
→ detailed user guide.

Load Root-Certificate / Revocation List (Deutsche Telekom Root CA 2)

The Fraunhofer Root CA has been certified by Deutsche Telekom AG. The corresponding root certificate of Deutsche Telekom is already contained in many operating systems, applications and browsers. If this is not the case (e. g. Mozilla Firefox / Thunderbird), you may download this certificate below.

→ Download root certificate
Deutsche Telek

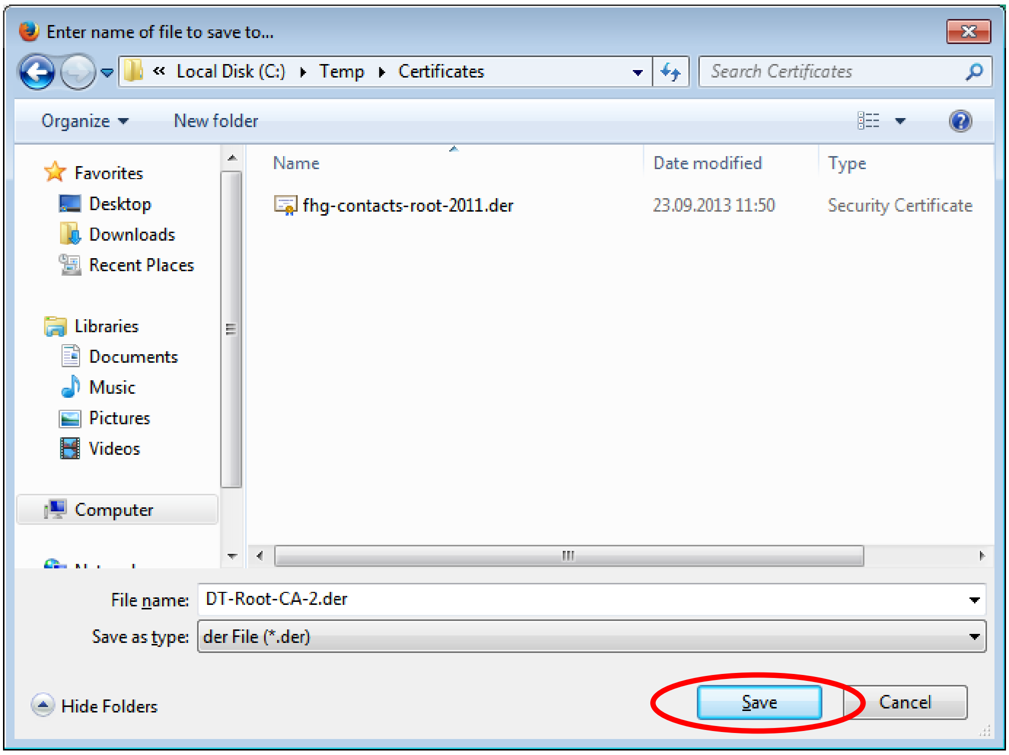
→ Download certificate revocation list
Deutsche Telekom Root CA 2

Control data for the root certificate c

- ***Distinguished Name:*** CN = Deu c Trust Center, O = Deutsche Telekom AG, C=DE
- ***Certificate issuer:*** identical, si
- ***Certificate valid period:*** 09.07
- ***SHA-1 Fingerprint:*** 85:A4:08:C 8C:DE:37:BF

Figure 39: Downloading the PKI for Fraunhofer Employees root certificate

Now select the folder that you want to save the certificate in and click **Save** (see Figure 40).



Enter name of file to save to...

Local Disk (C:) ▸ Temp ▸ Certificates

Name	Date modified	Type
fhg-contacts-root-2011.der	23.09.2013 11:50	Security Certificate

File name: DT-Root-CA-2.der

Save as type: der File (*.der)

Figure 40: Saving the PKI for Fraunhofer Employees root certificate

Note: The Intermediate Certification Authorities certificates of the PKI for Fraunhofer Employees (*Fraunhofer Root CA 2007* certificate and *Fraunhofer User CA 2007* certificate) can be downloaded in exactly the same way.

4.1.2.1 Incorporating the PKI for Fraunhofer Employees root certificate / certificate chain into the Microsoft certificate store

The method for integrating the PKI for Fraunhofer Employees root certificate (*Deutsche Telekom Root CA 2* certificate) into the Microsoft certificate store is exactly the same as the method described in section 4.1.1.1.

If the Intermediate Certification Authorities certificates of the PKI for Fraunhofer Employees are to be imported, these certificates (Fraunhofer Root CA 2007 certificate and Fraunhofer User CA 2007 certificate) should be imported into the *Intermediate Certification Authorities* certificate store instead of the *Trusted Root Certification* Authorities certificate store. Apart from this, integrating these certificates is done in exactly the same way as the method described in section 4.1.1.1.

4.1.2.2 Incorporating the PKI for Fraunhofer Employees root certificate / certificate chain into the Mozilla Thunderbird certificate manager

The method for integrating the PKI for Fraunhofer Employees root certificate (*Deutsche Telekom Root CA 2* certificate) or the Intermediate Certification Authorities certificates of the PKI for Fraunhofer Employees (*Fraunhofer Root CA 2007* certificate and *Fraunhofer User CA 2007* certificate) into the Mozilla Thunderbird certificate manager is exactly the same as the method described in section 4.1.1.2.

4.2 Incorporating your own personal certificate into the e-mail client

This section describes how to incorporate your personal certificate into your e-mail client and configure it in order to be able to send digitally signed e-mails. The process for incorporating and configuring personal certificates in your e-mail client varies depending on the e-mail client you use. For this reason this section describes the process for applications that access the Microsoft certificate store (such as Microsoft Outlook) as well as for applications that use their own certificate store (such as Mozilla Thunderbird).

4.2.1 Incorporating your own personal certificate into the Microsoft certificate store

If you use Microsoft Outlook for your e-mail communication, then your personal certificate must be imported into the Microsoft certificate store that the different versions of Microsoft Outlook also access.

Note: If you used Internet Explorer to request your own certificate on your system, there is no need to incorporate your personal certificate into the Microsoft certificate store. It will already have been added as part of the request process (see section 2.1). In this case it is necessary only to configure the certificate, for instance in Microsoft Outlook. The method for doing so is described in sections 4.2.1.1 ff.

Do so by opening the Microsoft certificate store via **Start → Control Panel → Network and Internet → Internet Options → Content → Certificates** and opening up the **Personal** tab. Click on **Import** (see Figure 41).

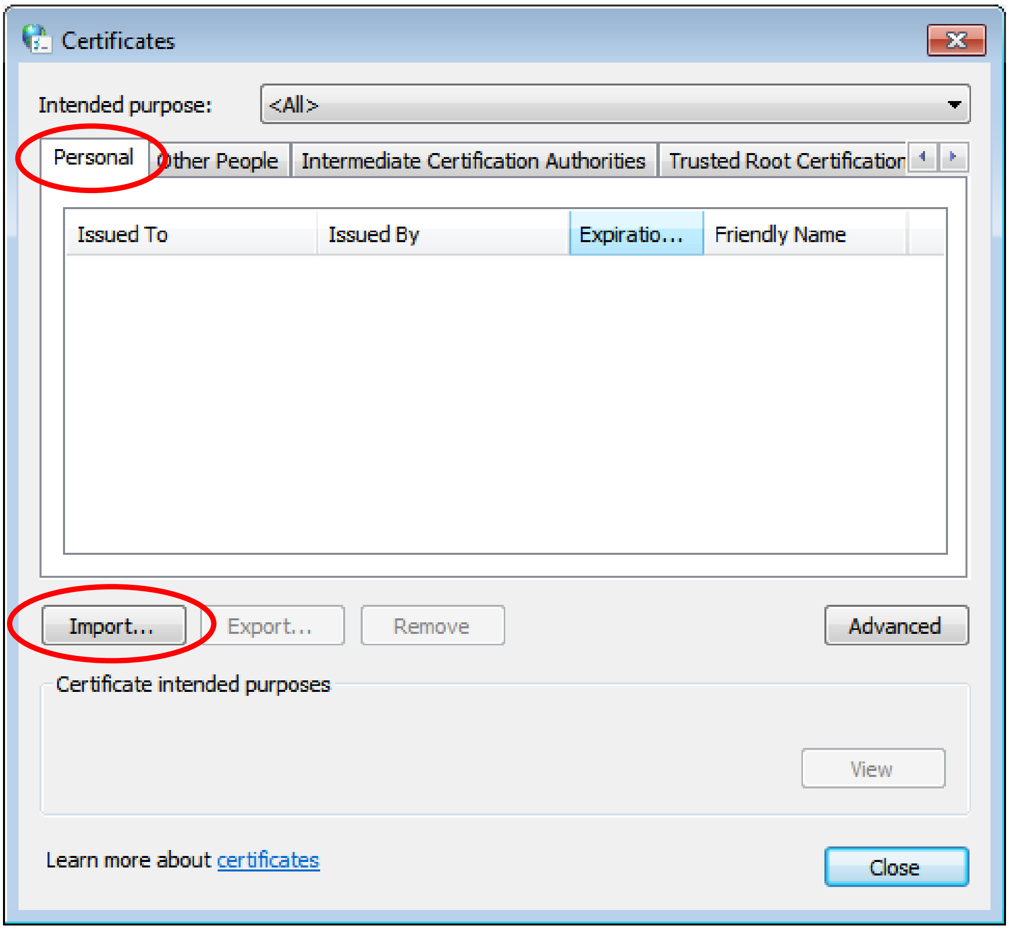


Figure 41: Screenshot showing *Personal Certificates* in the Microsoft certificate store

This opens the certificate import wizard. Confirm the first window by clicking **Next**. Now click the **Browse** button and select your certificate. Confirm the dialog window by clicking **Open** and then on **Next** (see Figure 42).

Note: To make sure your personal certificate is shown in the selection dialog window, you must change the filter that determines the file types shown from "X.509 Certificate (*.cer,*.crt)" to "Personal Information Exchange (*.pfx,*.p12)". Only then will you also be able to see files containing a corresponding private key as well as a certificate.

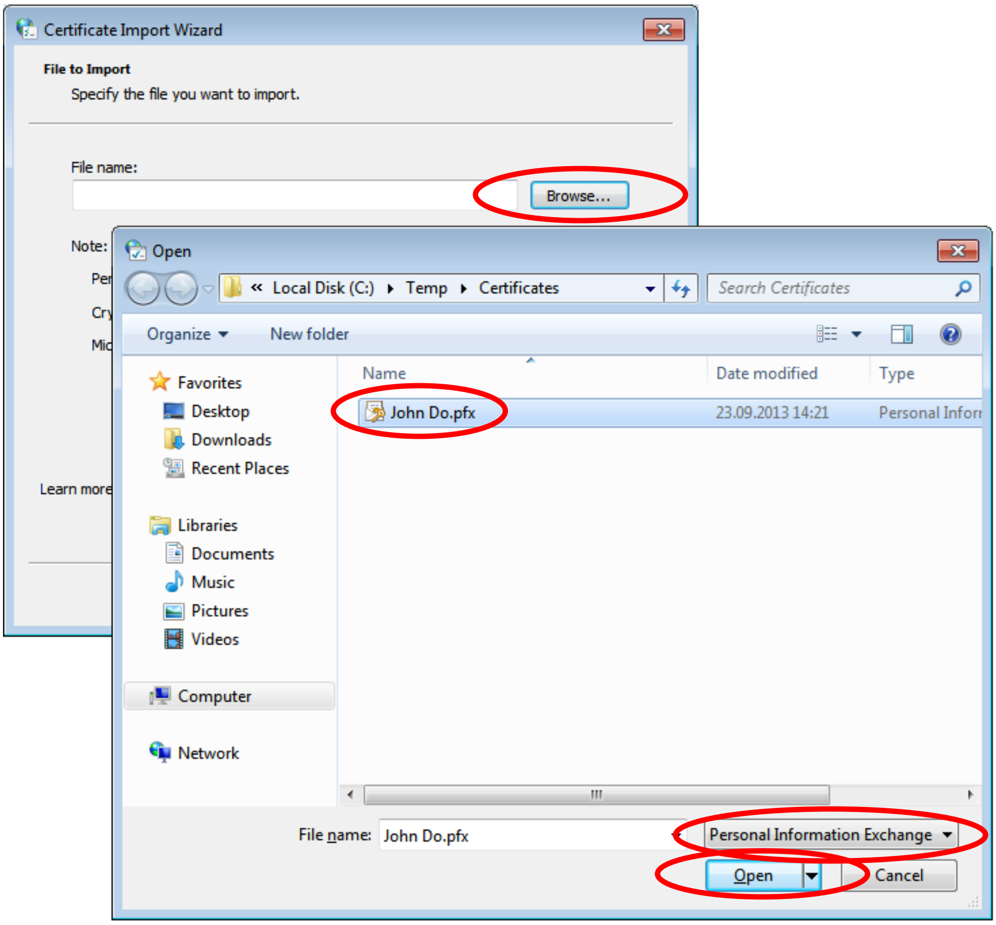
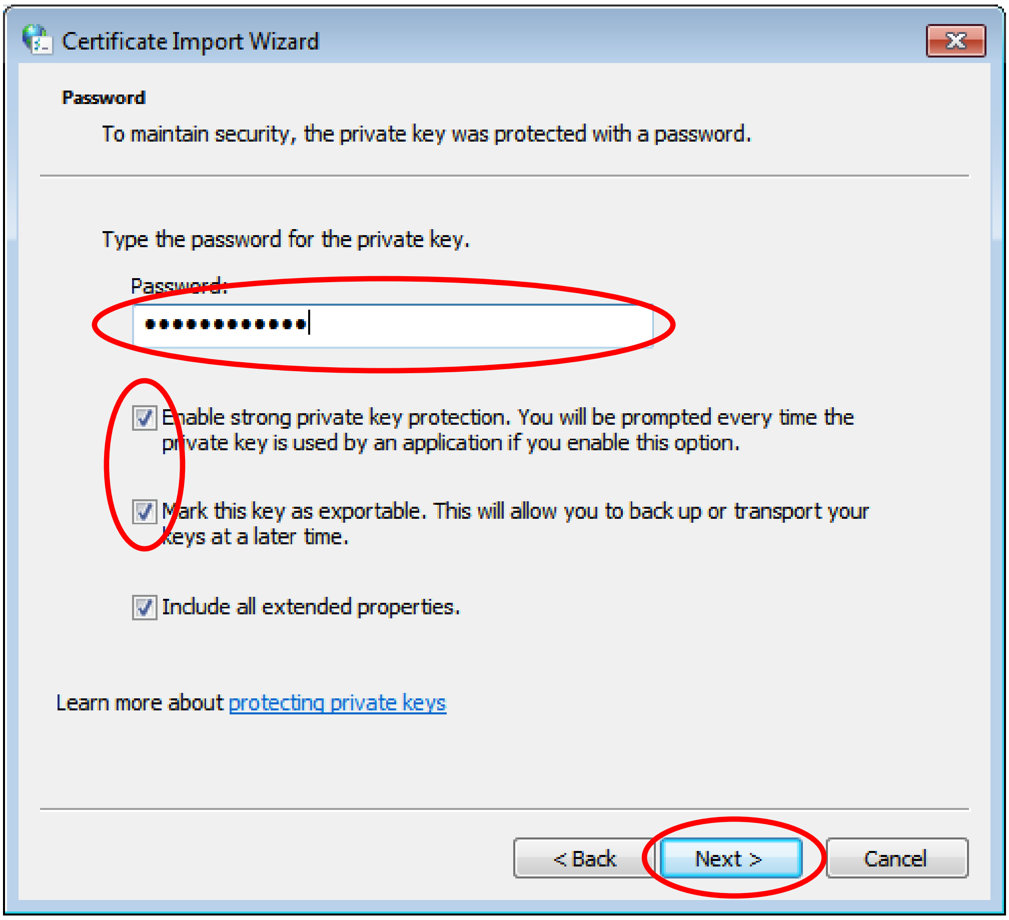


Figure 42: Selecting your personal certificate when importing it into the Microsoft certificate store

When you created and saved the certificate you will have set a password for the private key to prevent unauthorized access. Enter that password now. Select the **Mark this key as exportable** option and, if applicable, the **Enable strong private key protection** option in addition to the **Include all extended properties** option that is preselected by default (see Figure 43). By selecting **Mark this key as exportable** you ensure that your certificate and private key can be exported again later. Now click on **Next**.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password: ••••••••••••

☑ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

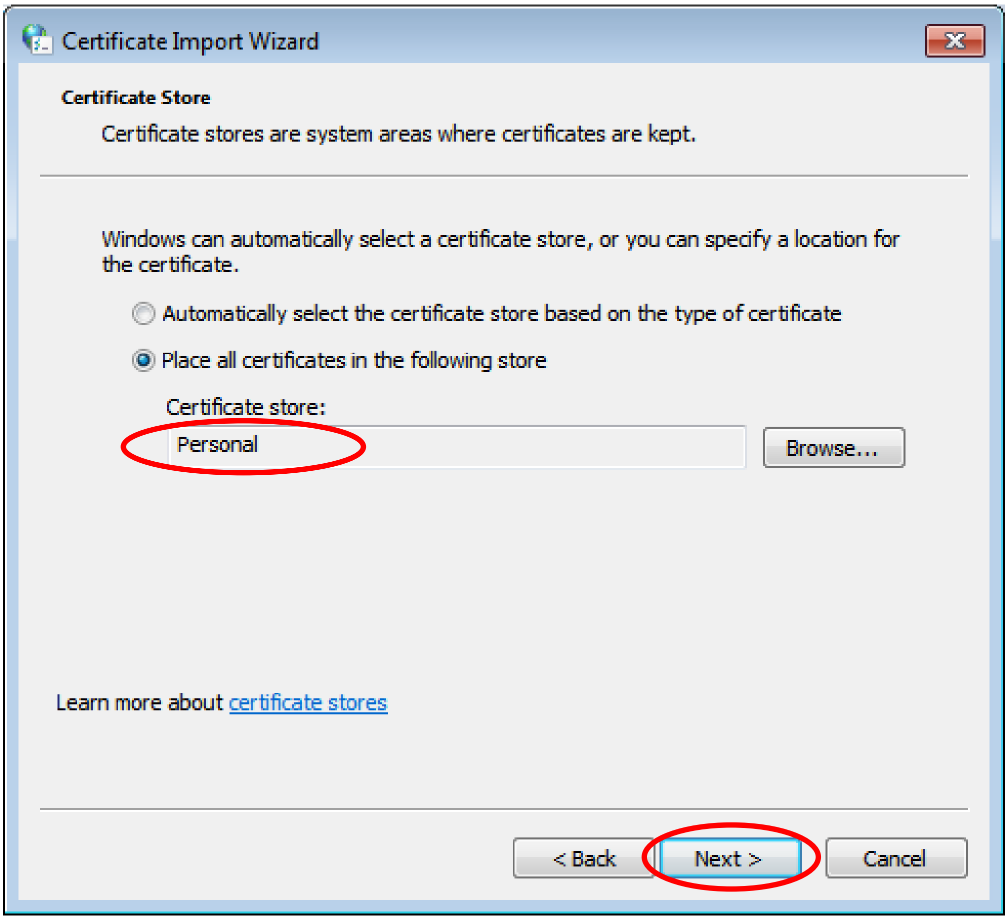
☑ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☑ Include all extended properties.

Learn more about protecting private keys

Figure 43: Entering the password and setting the import options when importing a personal certificate into the Microsoft certificate store

In the next dialog box, accept the default settings and confirm by clicking **Next** (see Figure 44).



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

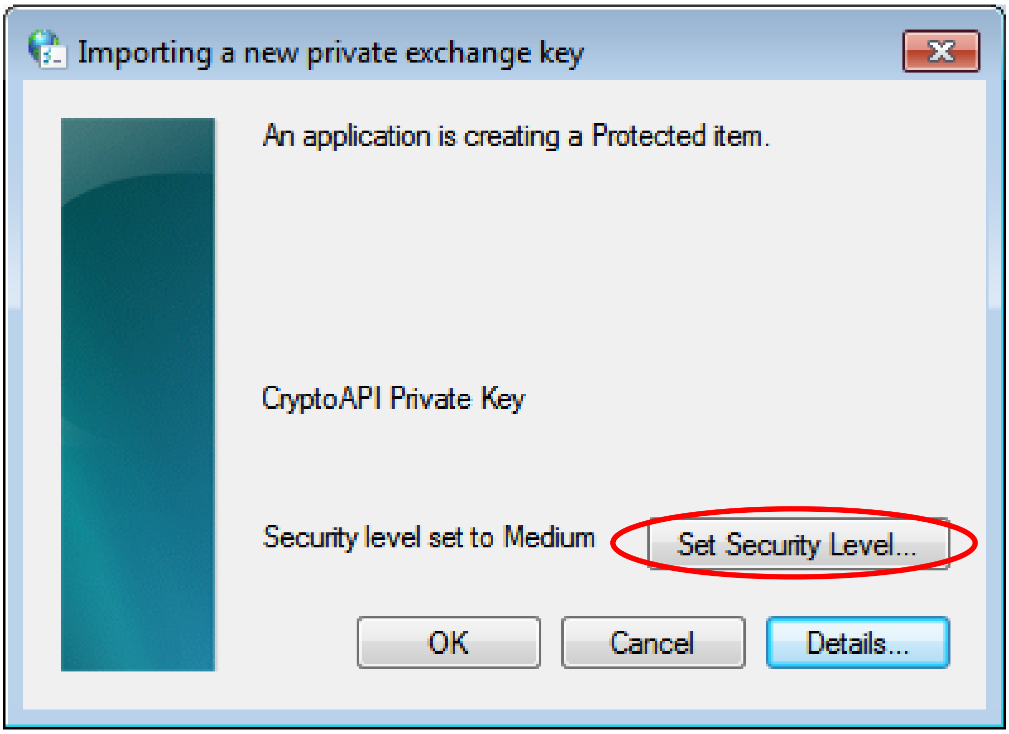
● Place all certificates in the following store

Certificate store: Personal

Figure 44: Selecting the certificate store to use when importing personal certificates into the Microsoft certificate store

You will now be presented with the **Completing the certificate import Wizard** dialog window summarizing the settings you have specified. By clicking **Finish** you give the final authorization for your personal certificate to be incorporated into the Microsoft certificate store. If you have selected the **Enable strong protection for the private key** option (see Figure 43), you will now be prompted to issue a password for instances when the private key is used in future. A series of dialog windows will assist you with this process. You will have to enter this password later, for instance every time you sign or decrypt an e-mail. Do this by first selecting **Set Security Level…** as shown in the dialog window in Figure 45.

Note: If you have not selected the **Enable strong private key protection** option (see Figure 43), the four dialog windows shown below are not relevant.



Importing a new private exchange key

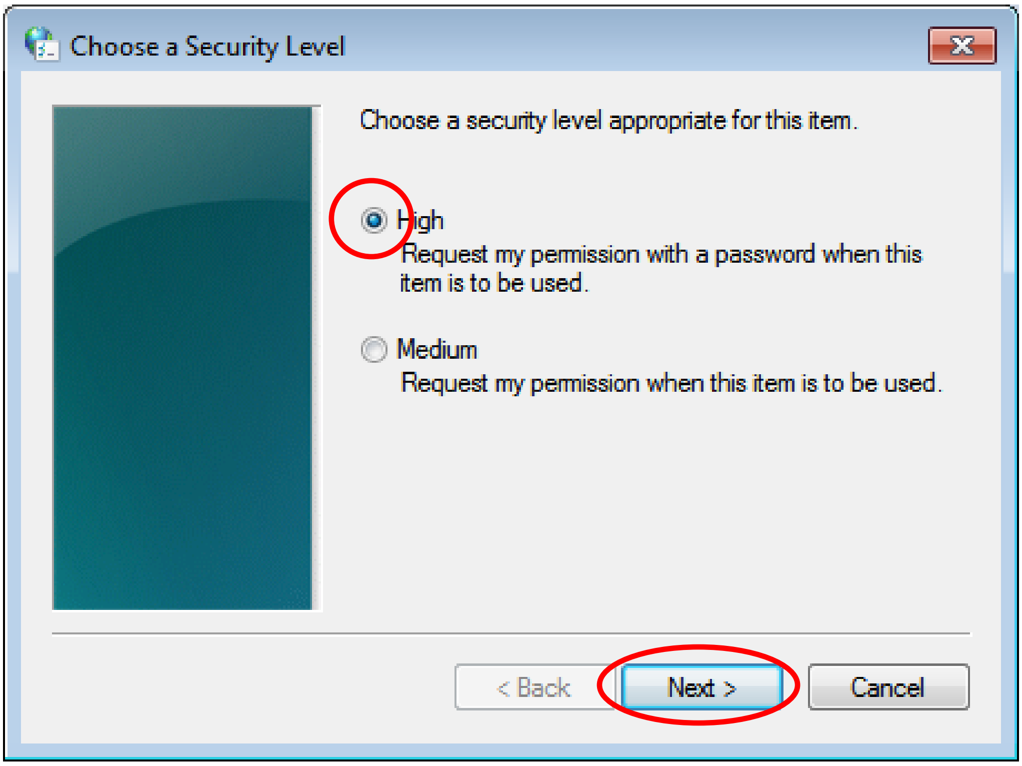
An application is creating a Protected item.

CryptoAPI Private Key

Security level set to Medium

Figure 45: Adjusting the security level for access to personal private keys at a later point when importing personal certificates into the Microsoft certificate store

First you will have to reconfirm that you wish to be prompted to enter a password every time you use the private key that goes with your certificate. To do so, change the private key security level from **Medium** to **High** and then exit the dialog window by clicking **Next** (see Figure 46).



Choose a Security Level

Choose a security level appropriate for this item.

● High
Request my permission with a password when this item is to be used.

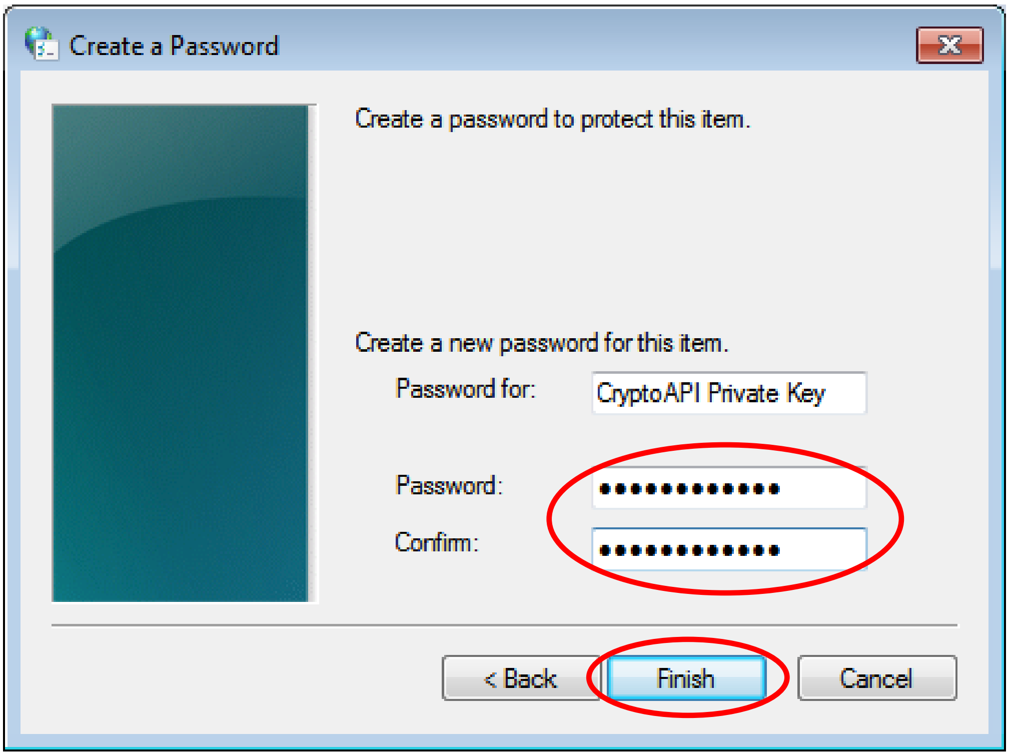
○ Medium
Request my permission when this item is to be used.

Figure 46: Changing the security level so that a password is requested whenever the user's private key is accessed at a later point

You will now be prompted to set the password that you wish to be asked for whenever the private key is used. For security reasons you must enter it twice. Complete the dialog window by clicking **Finish** (see Figure 47).

Note: The password you set at this point will be requested whenever an application needs to access your private key (for instance when digitally signing or decrypting e-mails). It does not have to be the same as the transport password for the key and certificate file that you entered in Figure 43. If you decide to issue another password, please choose one that is secure[3].

[3] The password should be at least twelve characters long and contain upper and lower case letters, numbers and symbols.



Create a Password

Create a password to protect this item.

Create a new password for this item.

Password for: CryptoAPI Private Key

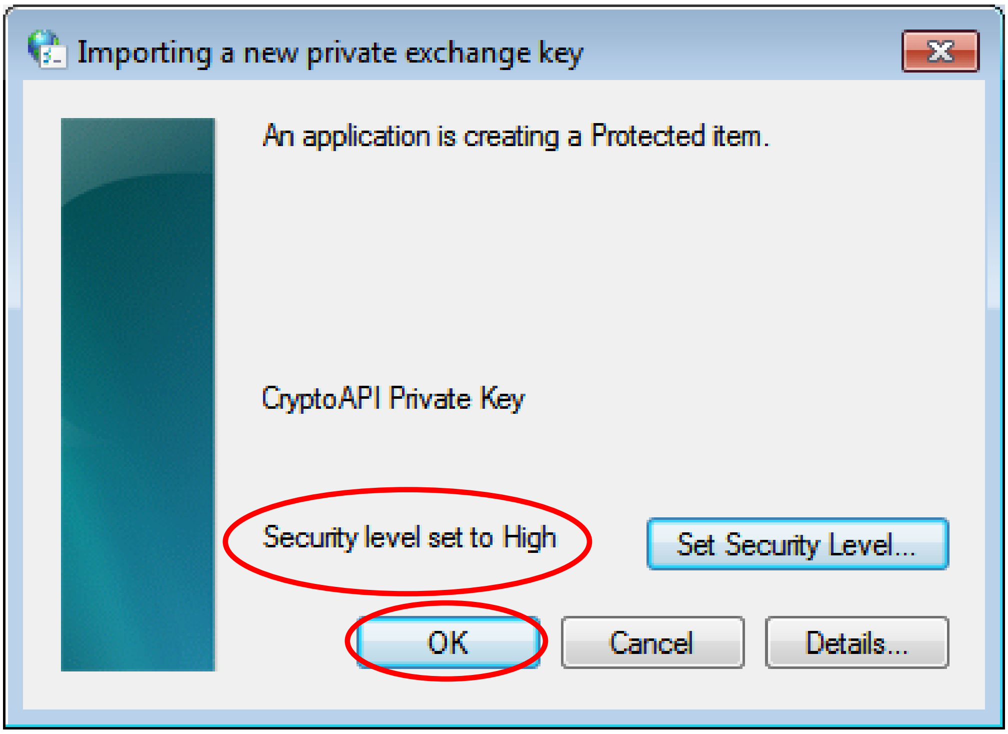
Password: ●●●●●●●●●●●●

Confirm: ●●●●●●●●●●●●

Figure 47: Setting the password for later access to the user's private key

Return to the dialog window that you are familiar with from Figure 45. The security level should now correspond to the level you selected (see Figure 48). Clicking **OK** imports your personal certificate and the private key associated with it into the Microsoft certificate store. The message shown in Figure 49 will appear to confirm the import. Confirm this dialog window by clicking **OK** too.

Your personal certificate is now available in the Microsoft certificate store and can be configured for secure e-mail communication, for example in Outlook (see Sections 4.2.1.1ff.).



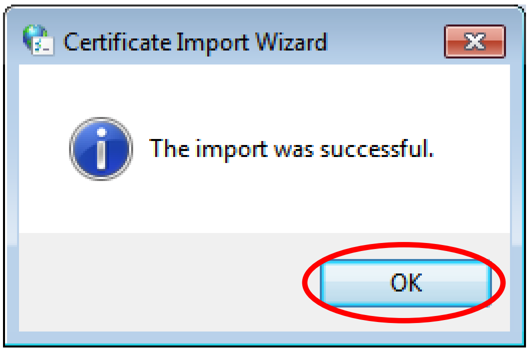
Importing a new private exchange key

An application is creating a Protected item.

CryptoAPI Private Key

Security level set to High

Figure 48: Adjusting the security level for access to personal private keys at a later point when importing personal certificates into the Microsoft certificate store



Certificate Import Wizard

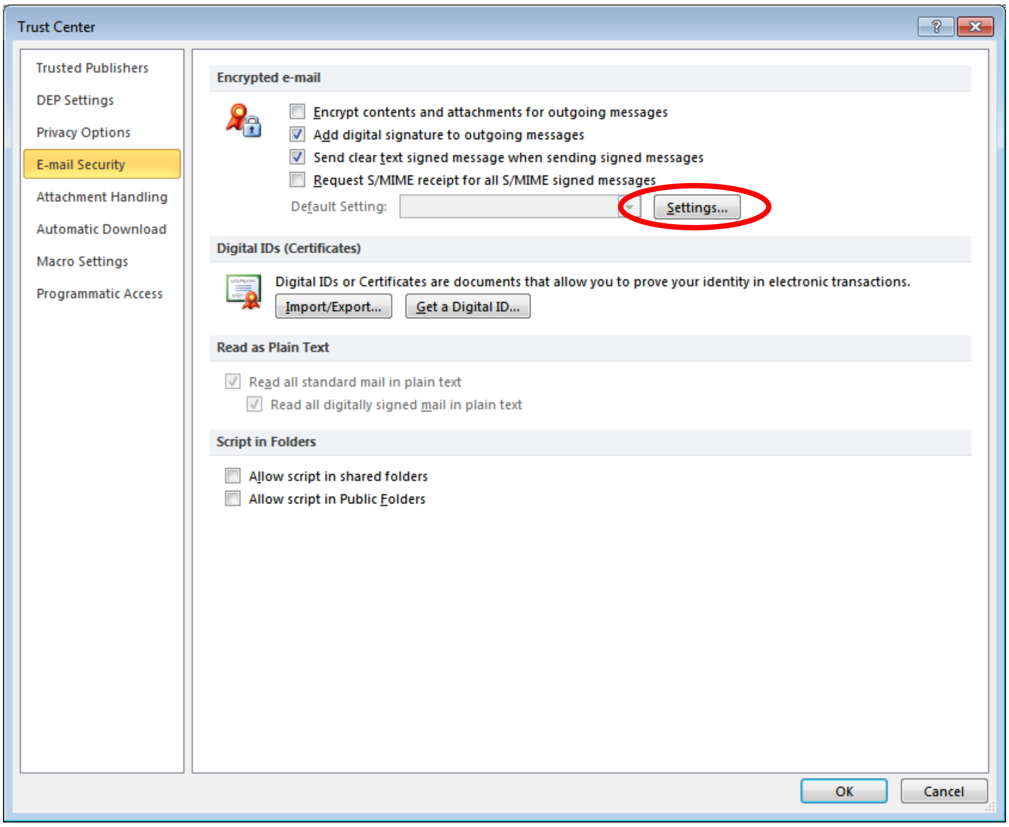
The import was successful.

Figure 49: Personal certificate and private key have been successfully imported into the Microsoft certificate store

4.2.1.1 Configuring your own personal certificate in Microsoft Outlook 2010

In order to inform Microsoft Outlook 2010 of the personal certificate and private key it should use to sign/decrypt e-mails, you must first configure the certificate in the e-mail client.

Begin by opening the **Trust Center** via **File → Options → Trust Center → Trust Center Settings … → E-mail Security**. Now click on the **Settings** button under "Encrypted e-mail" (see Figure 50).



Encrypted e-mail

□ Encrypt contents and attachments for outgoing messages
☑ Add digital signature to outgoing messages
☑ Send clear text signed message when sending signed messages
□ Request S/MIME receipt for all S/MIME signed messages

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Read as Plain Text

☑ Read all standard mail in plain text
☑ Read all digitally signed mail in plain text

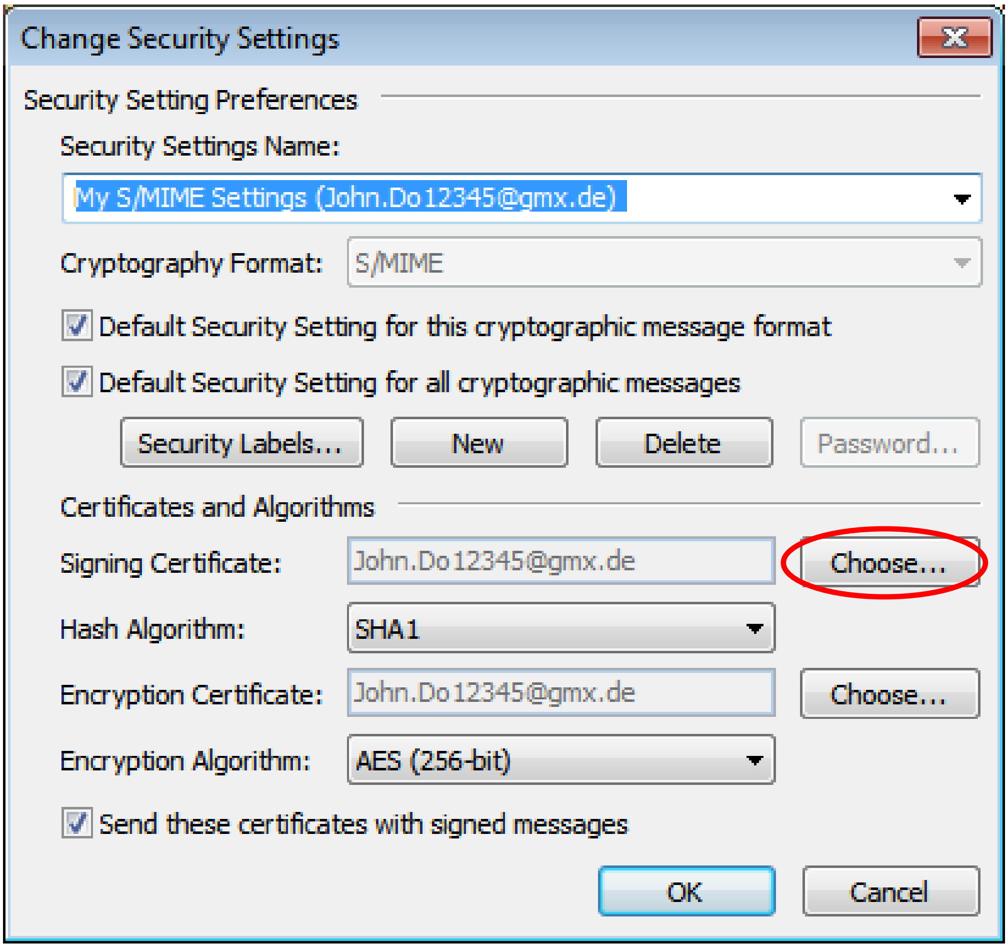
Script in Folders

□ Allow script in shared folders
□ Allow script in Public Folders

Figure 50: Outlook 2010 – Trust Center

This opens the "Change Security Settings" dialog window (see Figure 51). If applicable, change the name entered under **Security Settings Name** to one that matches your requirements, and click on the uppermost **Choose** button to set the signing certificate. You will be presented with a list of all certificates that have a "digital signature" function and for which you have a private key (as a general rule there is only one certificate of this kind available on your system). Select your own PKI for Fraunhofer Contacts personal certificate. This certificate will also automatically be entered as an encryption certificate, as it also has an encryption function. Now close all open dialog windows by clicking **OK**.

This concludes the process for configuring your own personal certificate in Microsoft Outlook 2010, meaning you are now able to send digitally signed e-mails and decrypt e-mails encrypted for your e-mail address.



Change Security Settings

Security Setting Preferences

Security Settings Name: My S/MIME Settings (John.Do12345@gmx.de)

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format

☑ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate: John.Do12345@gmx.de

Hash Algorithm: SHA1

Encryption Certificate: John.Do12345@gmx.de

Encryption Algorithm: AES (256-bit)

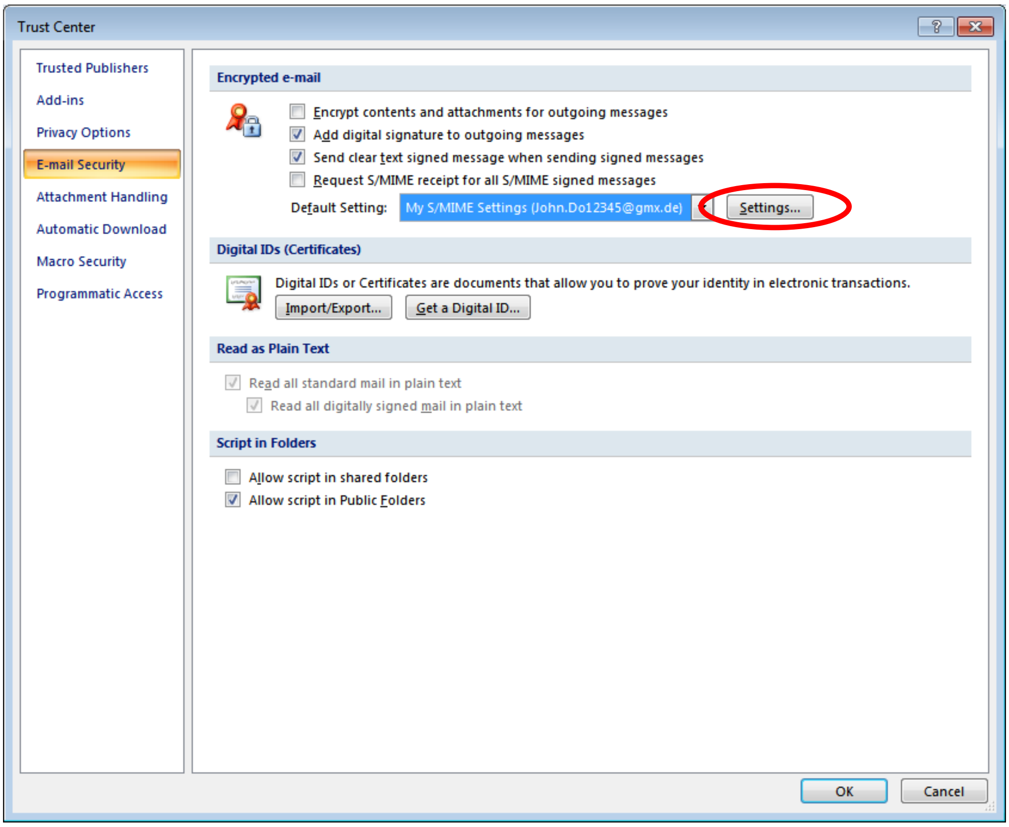
☑ Send these certificates with signed messages

Figure 51: Outlook 2010 – Configuring a personal certificate

4.2.1.2 Configuring your own personal certificate in Microsoft Outlook 2007

In order to inform Microsoft Outlook 2007 of the personal certificate and private key it should use to sign/decrypt e-mails, you must configure the certificate in the e-mail client.

Begin by opening the **Trust Center** via **Extras → Trust Center → E-Mail Security**. Now click on the **Settings** button under "Encrypted e-mail" (see Figure 52).



Encrypted e-mail

☐ Encrypt contents and attachments for outgoing messages
☑ Add digital signature to outgoing messages
☑ Send clear text signed message when sending signed messages
☐ Request S/MIME receipt for all S/MIME signed messages

Default Setting: My S/MIME Settings (John.Do12345@gmx.de)

Digital IDs (Certificates)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Read as Plain Text

☑ Read all standard mail in plain text
☑ Read all digitally signed mail in plain text

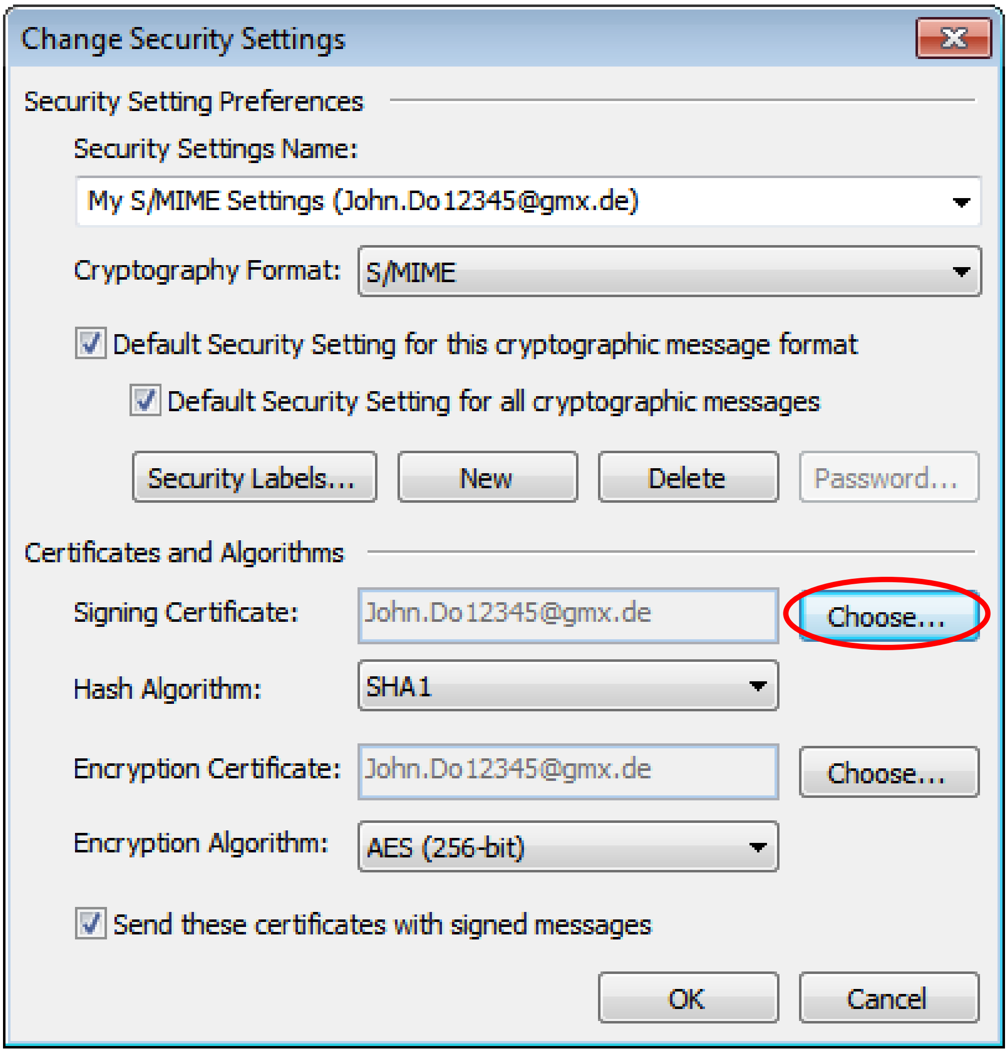
Script in Folders

☐ Allow script in shared folders
☑ Allow script in Public Folders

Figure 52: Outlook 2007 – Trust center

This opens the "Change Security Settings" dialog window (see Figure 53). Change or set the name entered under **Security Settings Name** to one that matches your requirements if necessary, and click on the uppermost **Choose** button to set the signing certificate. You will be presented with a list of all certificates that have a "digital signature" function and for which you have a private key (as a general rule there is only one certificate of this kind available on your system). Select your own PKI for Fraunhofer Contacts personal certificate. This certificate will also automatically be entered as an encryption certificate, as it also has an encryption function. Unless already selected by Outlook as a default setting, select the options **Default Security Setting for this cryptographic message format**, **Default Security Setting for all cryptographic messages** and **Send these certificates with signed messages**. Now close all open dialog windows by clicking **OK**.

This concludes the process for configuring your own personal certificate in Microsoft Outlook 2007, meaning you are now able to send digitally signed e-mails and decrypt e-mails encrypted for your e-mail address.



Change Security Settings

Security Setting Preferences

Security Settings Name: My S/MIME Settings (John.Do12345@gmx.de)

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format

☑ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate: John.Do12345@gmx.de

Hash Algorithm: SHA1

Encryption Certificate: John.Do12345@gmx.de

Encryption Algorithm: AES (256-bit)

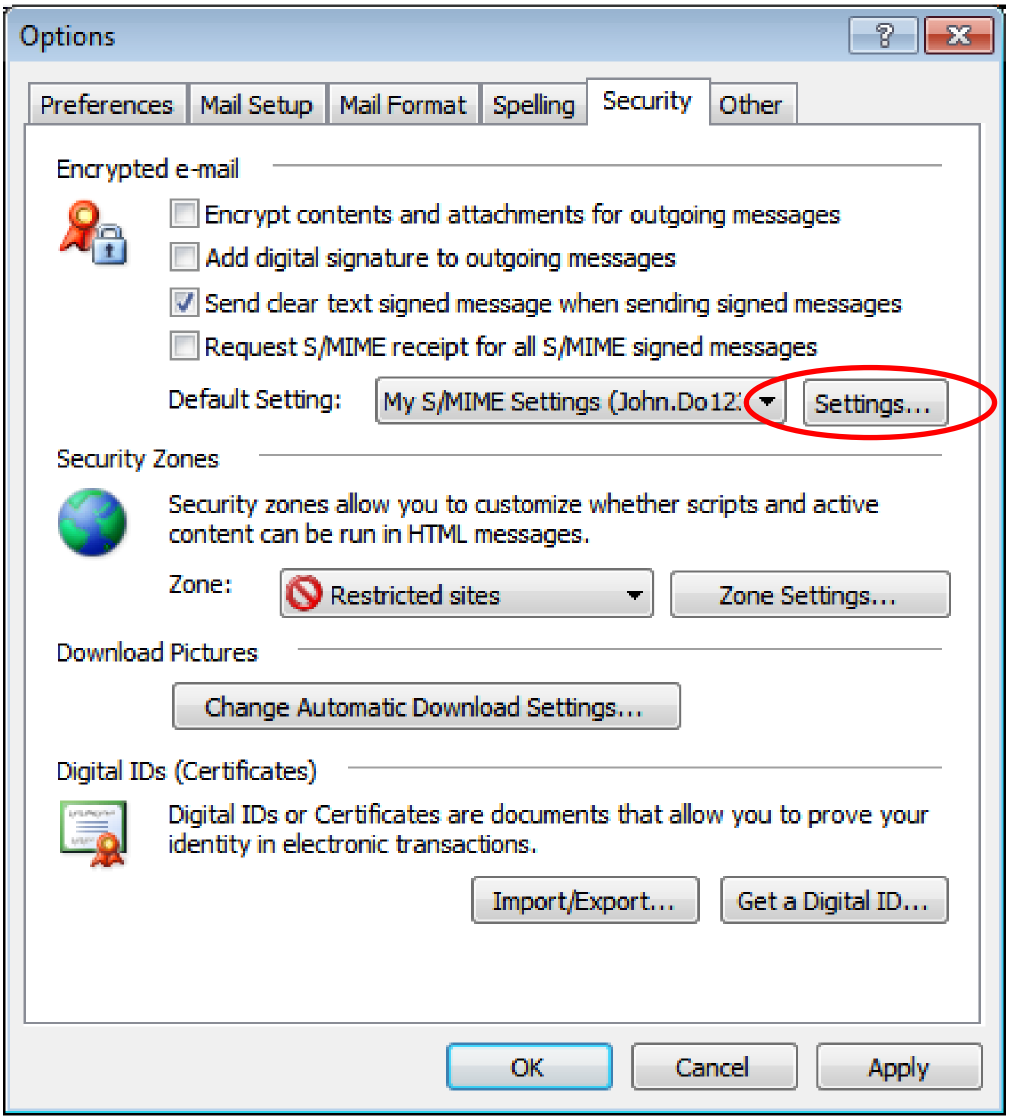
☑ Send these certificates with signed messages

Figure 53: Outlook 2007 – Configuring a personal certificate

4.2.1.3 Configuring your own personal certificate in Microsoft Outlook 2003

In order to inform Microsoft Outlook 2003 of the personal certificate and private key it should use to sign/decrypt e-mails, you must configure the certificate in the e-mail client.

Begin by opening the Outlook **S/MIME Options** via **Extras → Options**. Now select the **Security** tab and click on the **Settings** button under "Encrypted e-mail" (see Figure 54).



Encrypted e-mail

□ Encrypt contents and attachments for outgoing messages

□ Add digital signature to outgoing messages

☑ Send clear text signed message when sending signed messages

□ Request S/MIME receipt for all S/MIME signed messages

Default Setting: My S/MIME Settings (John.Do12:

Security Zones

Security zones allow you to customize whether scripts and active content can be run in HTML messages.

Zone: Restricted sites

Download Pictures

Digital IDs (Certificates)

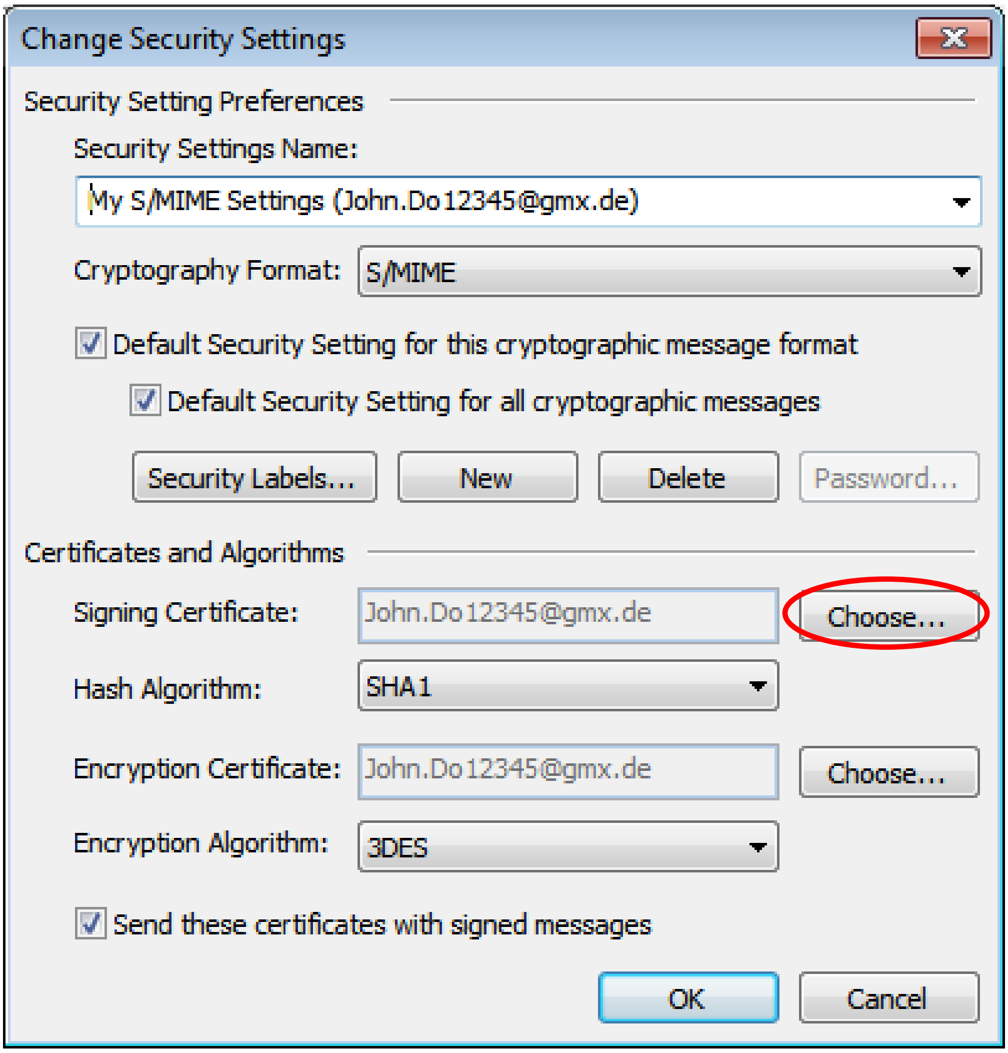
Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions.

Figure 54: Outlook 2003 – S/MIME options

This opens the "Change Security Settings" dialog window (see Figure 55). Change or set the name entered under **Security Settings Name** to one that matches your requirements if necessary, and click on the uppermost **Choose** button to set the signing certificate. You will be presented with a list of all certificates that have a "digital signature" function and for which you have a private key (as a general rule there is only one certificate of this kind available on your system). Select your own PKI for Fraunhofer Contacts personal certificate. This certificate will also automatically be entered as an encryption certificate, as it also has an encryption function. Unless already selected by Outlook as a default setting, select the options **Default Security Setting for this cryptographic message format**, **Default Security Setting for all cryptographic**

messages and **Send these certificates with signed messages**. Now close all open dialog windows by clicking **OK**.

This concludes the process for configuring your own personal certificate in Microsoft Outlook 2003, meaning you are now able to send digitally signed e-mails and decrypt e-mails encrypted for your e-mail address.



Change Security Settings

Security Setting Preferences

Security Settings Name: My S/MIME Settings (John.Do12345@gmx.de)

Cryptography Format: S/MIME

☑ Default Security Setting for this cryptographic message format

☑ Default Security Setting for all cryptographic messages

Certificates and Algorithms

Signing Certificate: John.Do12345@gmx.de

Hash Algorithm: SHA1

Encryption Certificate: John.Do12345@gmx.de

Encryption Algorithm: 3DES

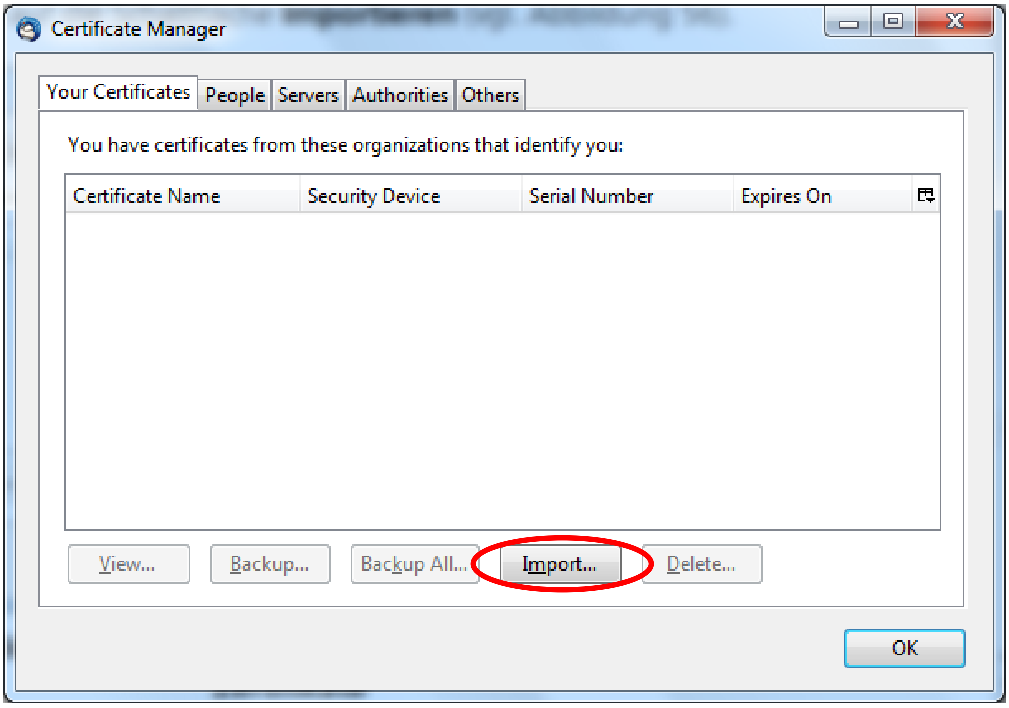
☑ Send these certificates with signed messages

Figure 55: Outlook 2003 – Configuring a personal certificate

4.2.2 Incorporating and configuring your own personal certificate in Mozilla Thunderbird

If you use Mozilla Thunderbird for your e-mail communication, then your personal certificate must be imported into the Mozilla Thunderbird certificate manager.

To import your personal certificate into the Thunderbird certificate manager, open the certificate manager via **Extras → Options → Advanced → Certificates → View Certificates** and open up the **Your Certificates** tab. Click on **Import** (see Figure 56).

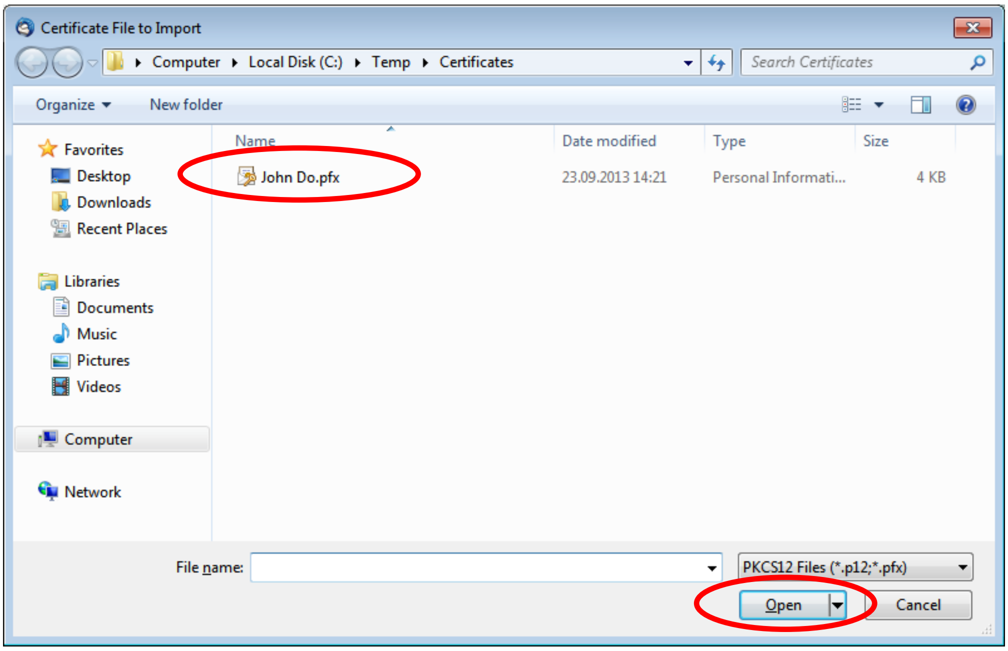


You have certificates from these organizations that identify you:

Certificate Name	Security Device	Serial Number	Expires On

Figure 56: Screenshot showing the Thunderbird *Your Certificates* certificate manager

This opens a file selection dialog window. Navigate to the location where you saved your PKI for Fraunhofer Contacts personal certificate and select it. Confirm the dialog window by clicking **Open** (see Figure 57).



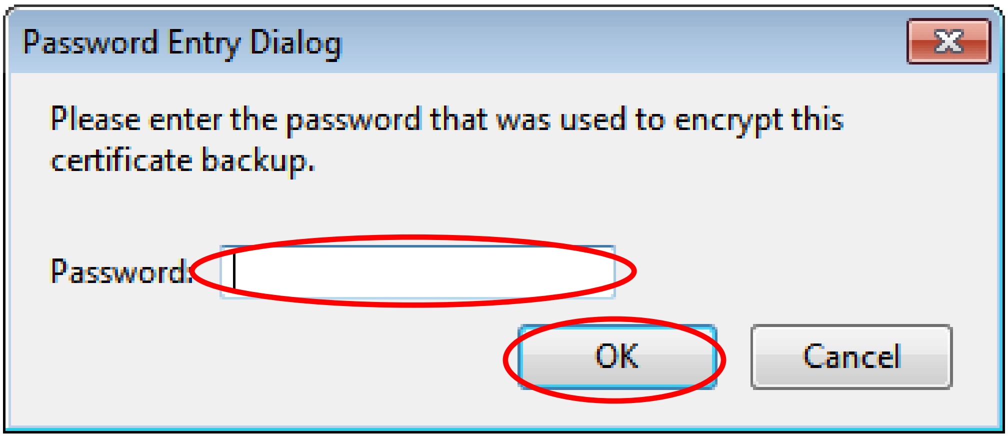
Name	Date modified	Type	Size
John Do.pfx	23.09.2013 14:21	Personal Informati...	4 KB

File name:

PKCS12 Files (*.p12;*.pfx)

Figure 57: Selecting your PKI for Fraunhofer Contacts personal certificate when importing it into the Thunderbird certificate manager

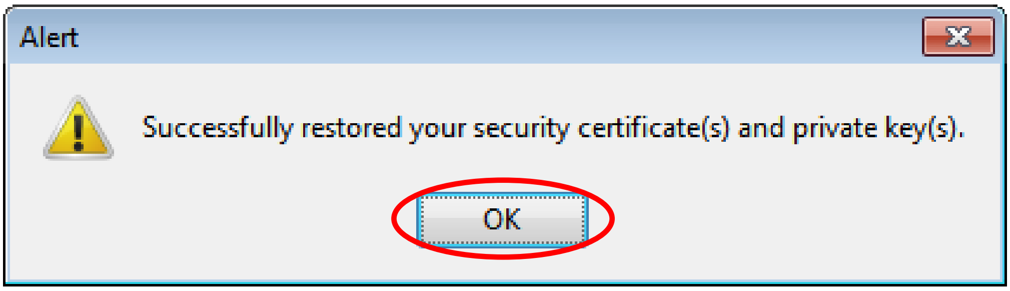
Now enter the password that you set when saving the certificate and private key to protect them against unauthorized access. Then click **OK** (see Figure 58).



Please enter the password that was used to encrypt this certificate backup.

Figure 58: Entering the password for your PKI for Fraunhofer Contacts personal certificate when importing it into the Thunderbird certificate manager

Once your certificate and private key have been successfully imported you will receive a confirmation message (see Figure 59). Click on **OK**. This concludes the process for importing your own personal certificate into Mozilla Thunderbird, meaning you can now configure the certificate for secure e-mail communication to then be able to sign and decrypt e-mails.

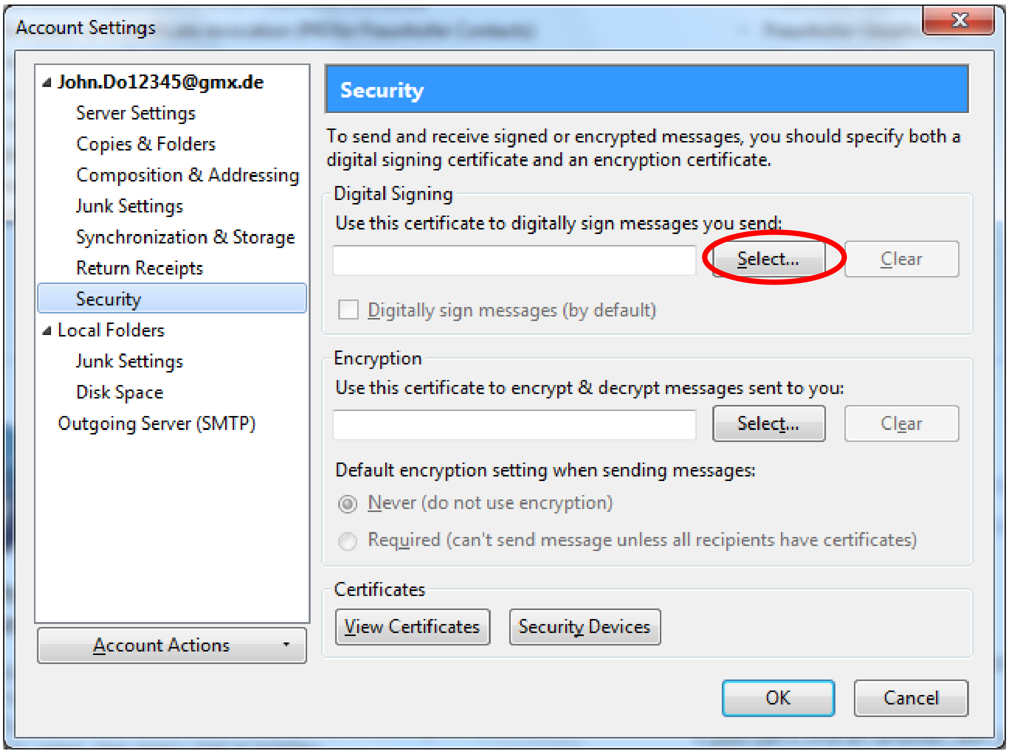


Alert

Successfully restored your security certificate(s) and private key(s).

Figure 59: Personal certificate and private key have been successfully imported into the Thunderbird certificate manager

Begin by opening **S/MIME Security** via **Extras → Account Settings → Security** (see Figure 60). Click on the uppermost **Select** button to set the signing certificate.



Account Settings

Security

To send and receive signed or encrypted messages, you should specify both a digital signing certificate and an encryption certificate.

Digital Signing

Use this certificate to digitally sign messages you send:

□ Digitally sign messages (by default)

Encryption

Use this certificate to encrypt & decrypt messages sent to you:

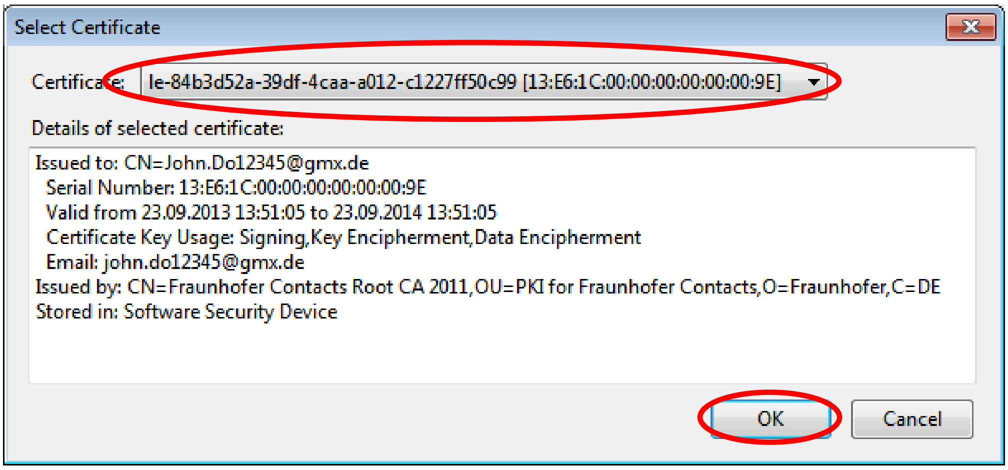
Default encryption setting when sending messages:

● Never (do not use encryption)

○ Required (can't send message unless all recipients have certificates)

Figure 60: Mozilla-Thunderbird – Selecting S/MIME settings

You will be presented with a list of all certificates that have a “digital signature” function and for which you have a private key (as a general rule there is only one certificate of this kind available on your system). Select your own PKI for Fraunhofer Contacts personal certificate and close the dialog window by clicking **OK** (see Figure 61).



Select Certificate

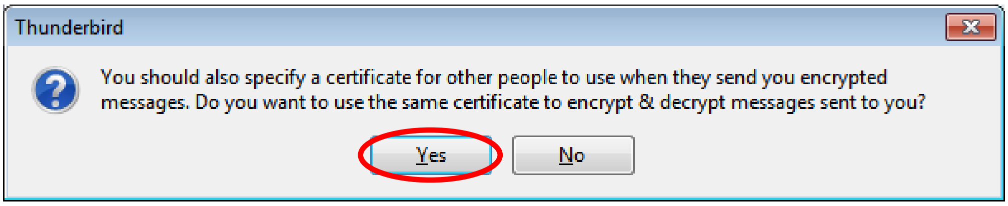
Certificate: le-84b3d52a-39df-4caa-a012-c1227ff50c99 [13:E6:1C:00:00:00:00:00:00:9E]

Details of selected certificate:

Issued to: CN=John.Do12345@gmx.de
Serial Number: 13:E6:1C:00:00:00:00:00:00:9E
Valid from 23.09.2013 13:51:05 to 23.09.2014 13:51:05
Certificate Key Usage: Signing,Key Encipherment,Data Encipherment
Email: john.do12345@gmx.de
Issued by: CN=Fraunhofer Contacts Root CA 2011,OU=PKI for Fraunhofer Contacts,O=Fraunhofer,C=DE
Stored in: Software Security Device

Figure 61: Mozilla Thunderbird – Setting up a signing certificate

You will then be asked whether you also wish to use this certificate to decrypt e-mails. Confirm this by clicking **Yes** (see Figure 62).



Thunderbird

You should also specify a certificate for other people to use when they send you encrypted messages. Do you want to use the same certificate to encrypt & decrypt messages sent to you?

Figure 62: Mozilla Thunderbird – Setting up a signing certificate

Now close all open dialog windows by clicking **OK**. This concludes the process for configuring your own personal certificate in Mozilla Thunderbird, meaning you are now able to send digitally signed e-mails and decrypt e-mails encrypted for your e-mail address.

4.3 Incorporating a Fraunhofer employee's certificate into the e-mail client

Note: As a general rule it is not necessary to incorporate a Fraunhofer employee's certificate into the e-mail client, as this happens automatically as soon as you receive and reply to a signed e-mail from a Fraunhofer employee. If you have come by the certificate another way, you can import it into various e-mail clients as described in the following subsections.

4.3.1 Incorporating a Fraunhofer employee’s certificate into Microsoft Outlook 2010

Begin by opening a new e-mail from the **Start** tab by clicking **New E-mail**. Enter the e-mail address of the Fraunhofer employee in the recipient field. Right-click on this e-mail address and select **“Add to Outlook Contacts”** from the context window (see Figure 63).

Note: If the Fraunhofer employee is already saved in your list of contacts, select **Look Up Outlook Contact** and open their contact details.

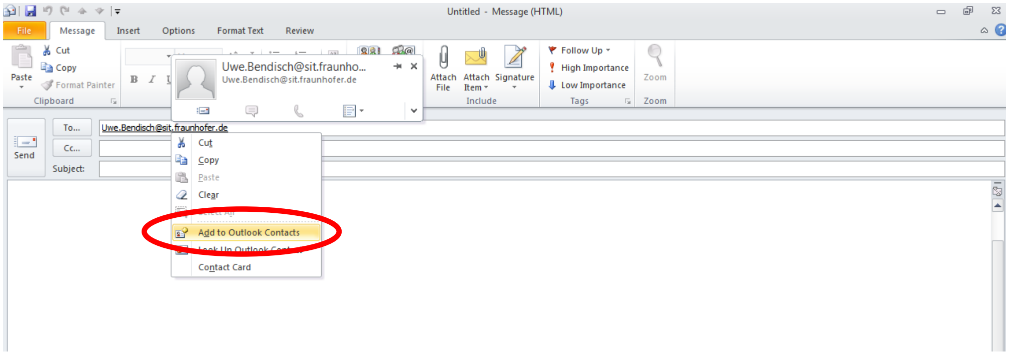
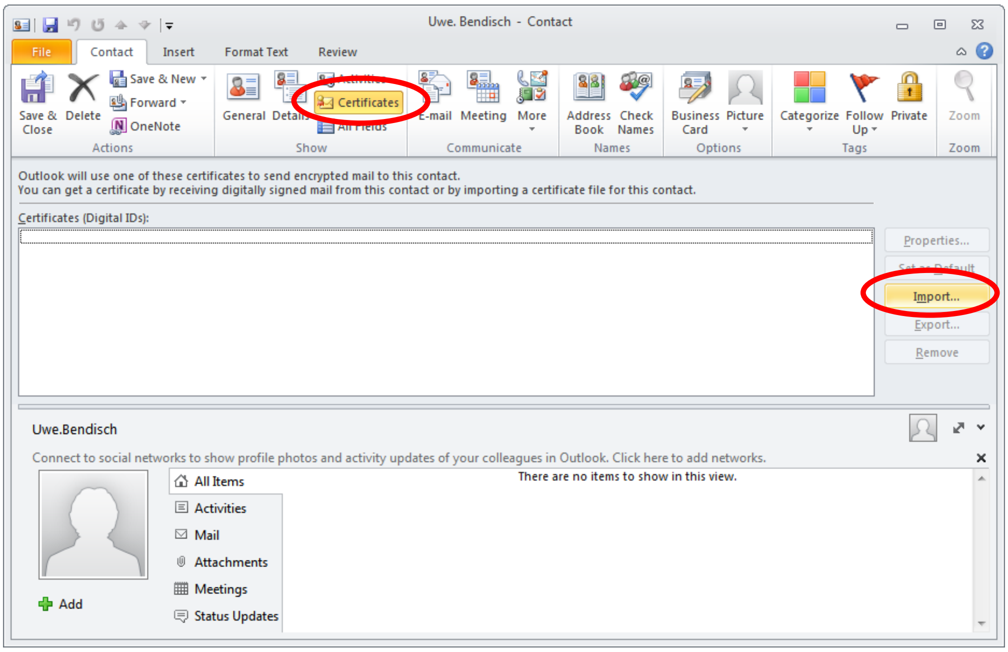


Figure 63: Adding a Fraunhofer employee as a contact in Outlook 2010

You will now be shown the contact details for this contact. Select **Certificates** in the **Contact** tab and click on **Import** (see Figure 64).



Outlook will use one of these certificates to send encrypted mail to this contact.
You can get a certificate by receiving digitally signed mail from this contact or by importing a certificate file for this contact.

Certificates (Digital IDs):

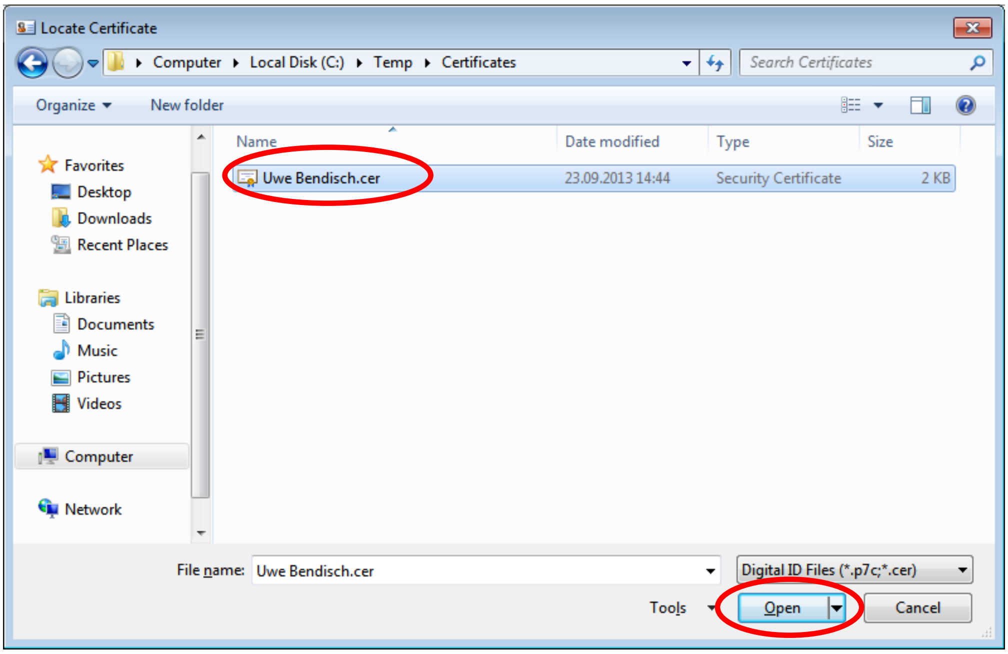
Uwe.Bendisch

Connect to social networks to show profile photos and activity updates of your colleagues in Outlook. Click here to add networks.

There are no items to show in this view.

Figure 64: Importing the Fraunhofer employee's certificate into Outlook 2010

Now go to the directory where you saved the Fraunhofer employee's certificate and select it. Click **Open** (see Figure 65).



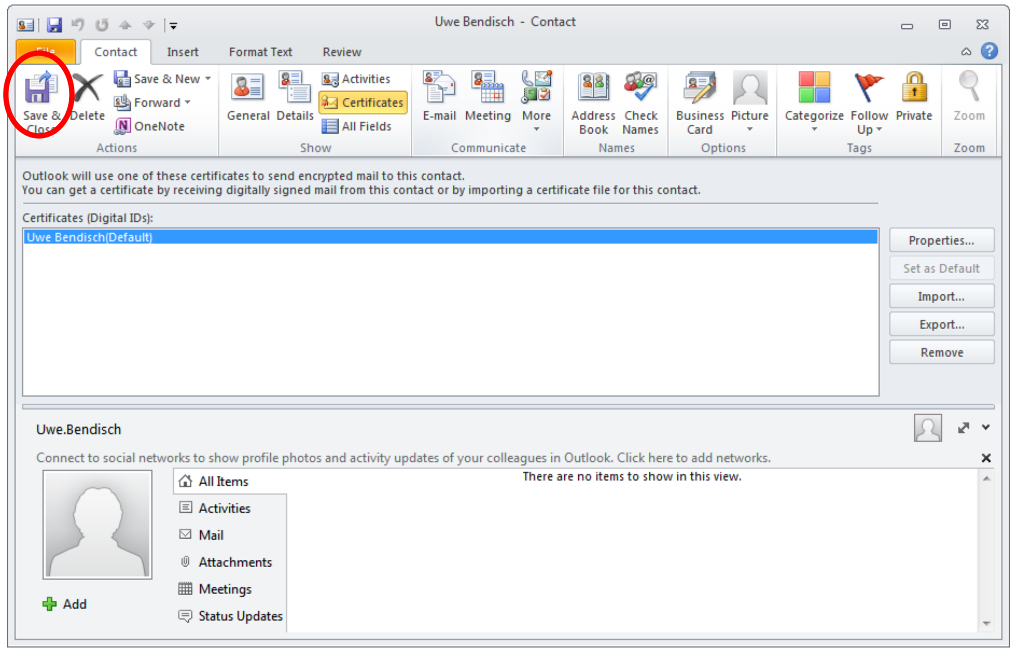
Name	Date modified	Type	Size
Uwe Bendisch.cer	23.09.2013 14:44	Security Certificate	2 KB

File name: Uwe Bendisch.cer

Digital ID Files (*.p7c;*.cer)

Figure 65: Selecting the Fraunhofer employee's certificate

The certificate has now been added to the certificate store. Now click on **Save & Close** (see Figure 66).



Outlook will use one of these certificates to send encrypted mail to this contact.
You can get a certificate by receiving digitally signed mail from this contact or by importing a certificate file for this contact.

Certificates (Digital IDs):

Uwe Bendisch(Default)

Uwe.Bendisch

Connect to social networks to show profile photos and activity updates of your colleagues in Outlook. Click here to add networks.

There are no items to show in this view.

Figure 66: Saving the certificate allocation in Outlook 2010

This concludes the process for integrating the Fraunhofer employee’s certificate into Outlook 2010, meaning the certificate can be used for secure e-mail communication.

4.3.2 Incorporating a Fraunhofer employee’s certificate into Microsoft Outlook 2007

Begin by opening a new e-mail from the **Start** tab by clicking **New E-mail**. Enter the e-mail address of the Fraunhofer employee in the recipient field. Right-click on this e-mail address and select **“Add to Outlook Contacts”** from the context window (see Figure 67).

Note: If the Fraunhofer employee is already saved in your list of contacts, select **Look Up Outlook Contact** and open their contact details.

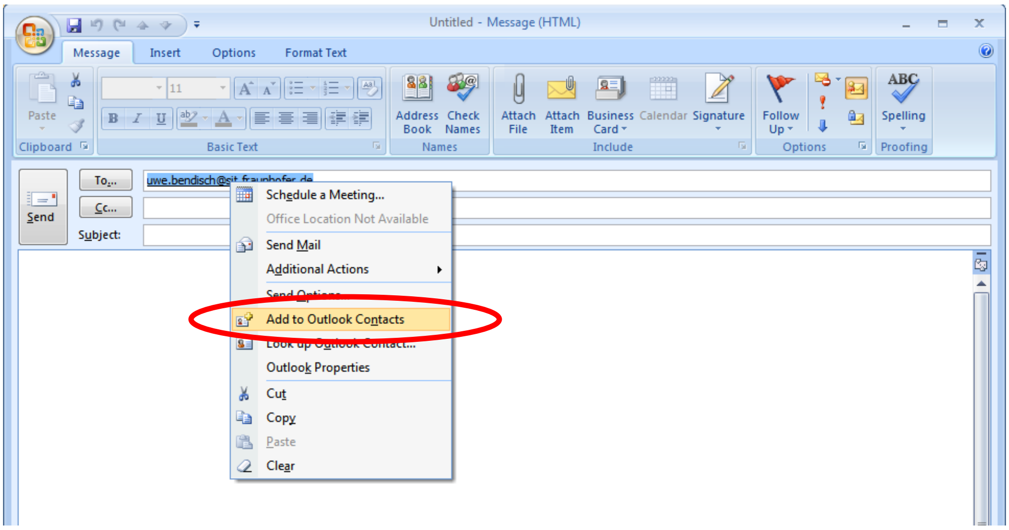
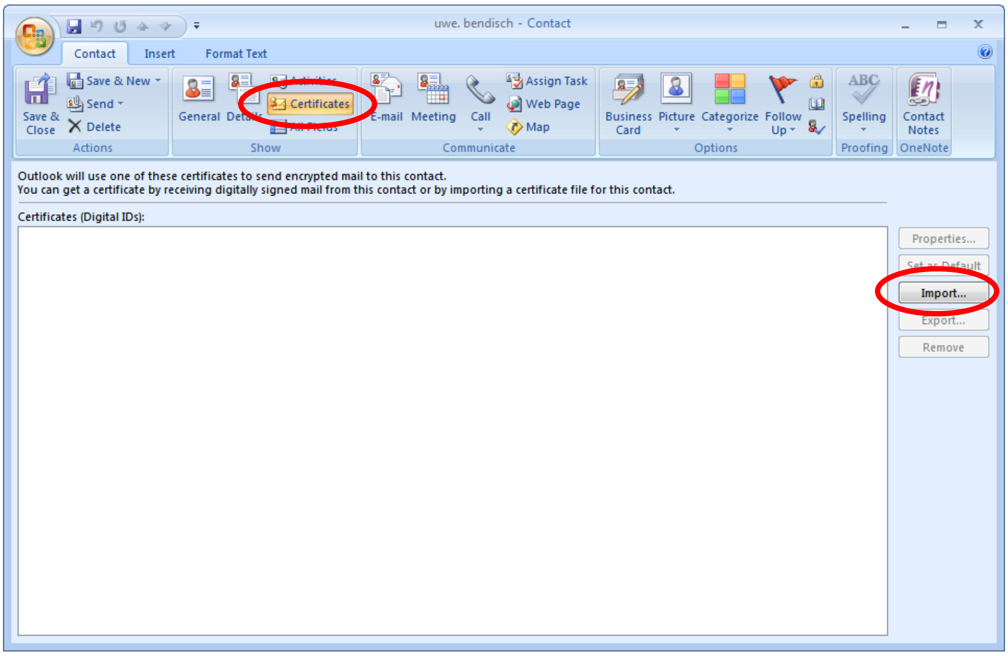


Figure 67: Adding a Fraunhofer employee as a contact in Outlook 2007

You will now be shown the contact details for this contact. Select **Certificates** in the **Contact** tab and click on **Import** (see Figure 68).

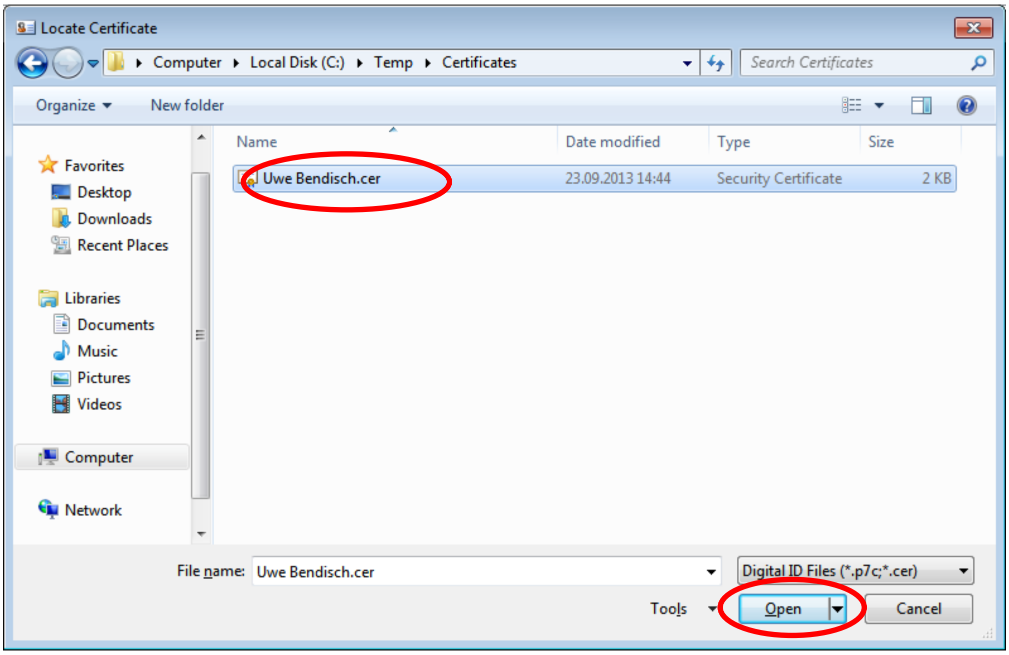


Outlook will use one of these certificates to send encrypted mail to this contact.
You can get a certificate by receiving digitally signed mail from this contact or by importing a certificate file for this contact.

Certificates (Digital IDs):

Figure 68: Importing the Fraunhofer employee’s certificate into Outlook 2007

Now go to the directory where you saved the Fraunhofer employee’s certificate and select it. Click **Open** (see Figure 69).



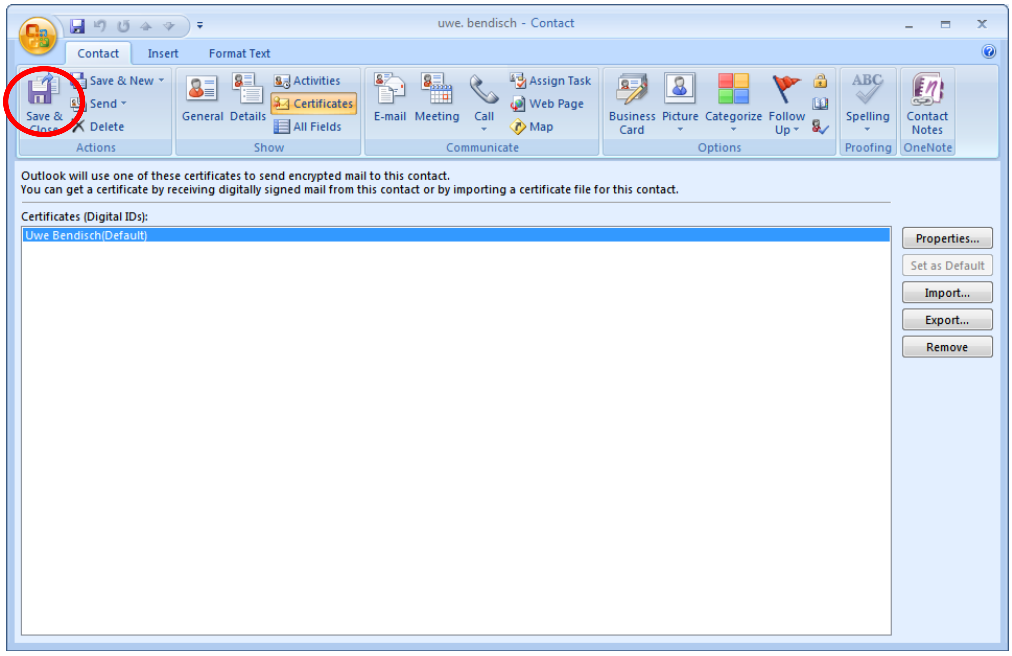
Name	Date modified	Type	Size
Uwe Bendisch.cer	23.09.2013 14:44	Security Certificate	2 KB

File name: Uwe Bendisch.cer

Digital ID Files (*.p7c;*.cer)

Figure 69: Selecting the Fraunhofer employee's certificate

The certificate has now been added to the certificate store. Now click on **Save & Close** (see Figure 70).



Outlook will use one of these certificates to send encrypted mail to this contact.
You can get a certificate by receiving digitally signed mail from this contact or by importing a certificate file for this contact.

Certificates (Digital IDs):

Uwe Bendisch(Default)

Figure 70: Saving the certificate allocation in Outlook 2007

This concludes the process for integrating the Fraunhofer employee's certificate into Outlook 2007, meaning the certificate can be used for secure e-mail communication.

4.3.3 Incorporating a Fraunhofer employee's certificate into Microsoft Outlook 2003

Begin by opening a new e-mail from the **Start** tab by clicking **New E-mail**. Enter the e-mail address of the Fraunhofer employee in the recipient field. Right-click on this e-mail address and select **"Add to Outlook Contacts"** from the context window (see Figure 71).

Note: If the Fraunhofer employee is already saved in your list of contacts, select **Look Up Outlook Contact** and open their contact details.

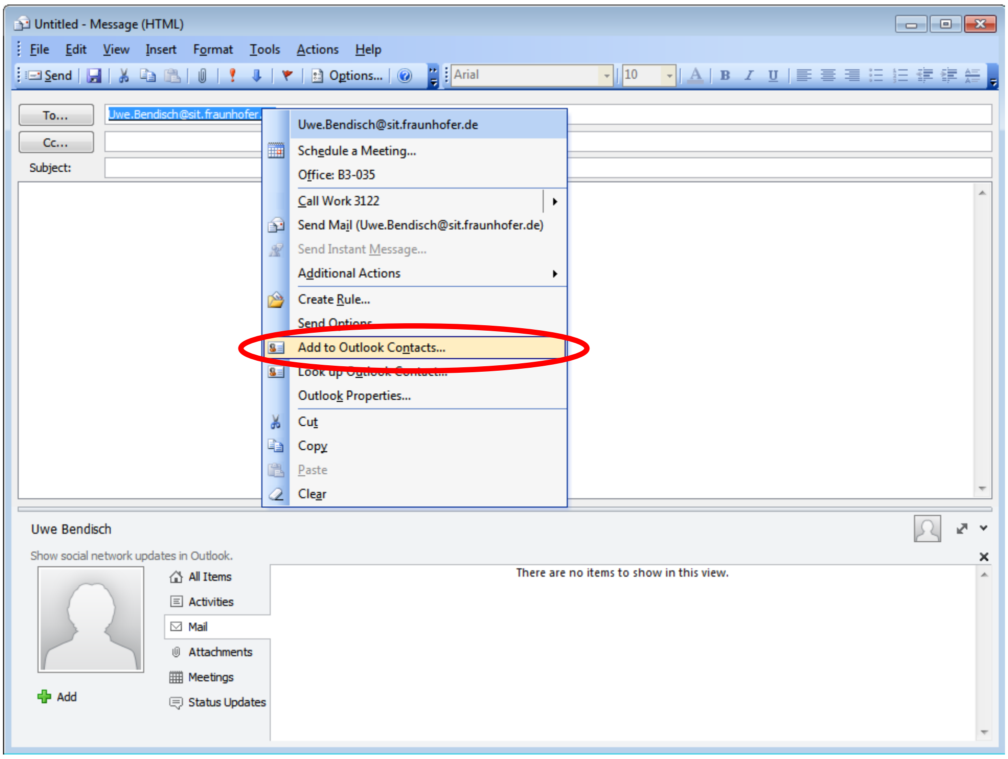
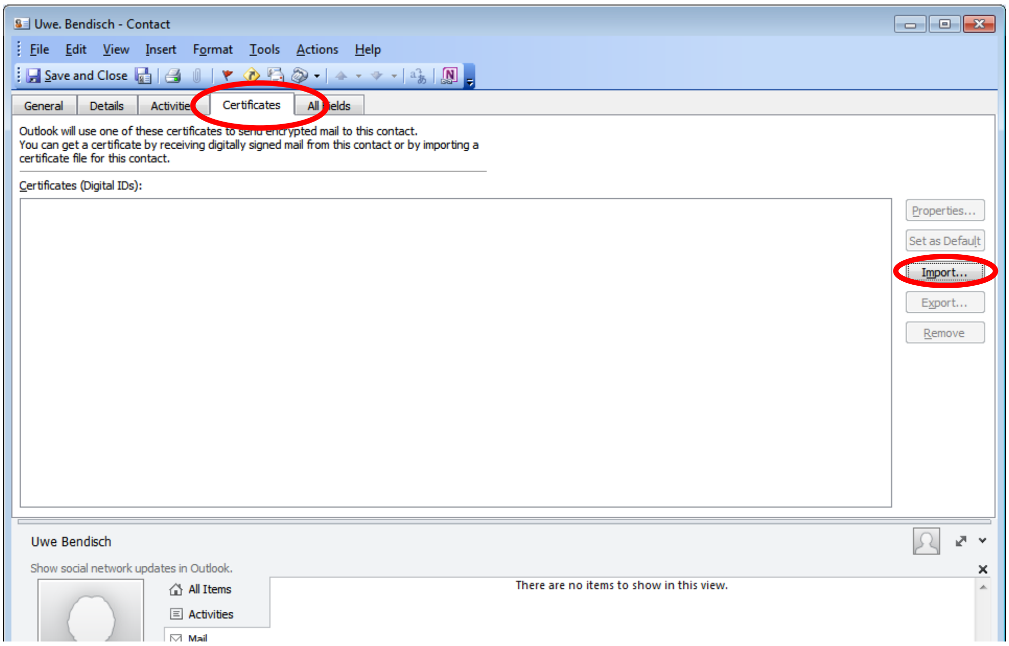

Untitled - Message (HTML)
File Edit View Insert Format Tools Actions Help
Send
Options...
Arial
10
To...
Cc...
Subject:
Uwe.Bendisch@sit.fraunhofer.
Uwe.Bendisch@sit.fraunhofer.de
Schedule a Meeting...
Office: B3-035
Call Work 3122
Send Mail (Uwe.Bendisch@sit.fraunhofer.de)
Send Instant Message...
Additional Actions
Create Rule...
Send Options
Add to Outlook Contacts...
Look up Outlook Contact...
Outlook Properties...
Cut
Copy
Paste
Clear
Uwe Bendisch
Show social network updates in Outlook.
All Items
Activities
Mail
Attachments
Meetings
Status Updates
Add
There are no items to show in this view.

Figure 71: Adding a Fraunhofer employee as a contact in Outlook 2003

You will now be shown the contact details for this contact. Select **Certificates** in the **Contact** tab and click on **Import** (see Figure 72).



Outlook will use one of these certificates to send encrypted mail to this contact.
You can get a certificate by receiving digitally signed mail from this contact or by importing a certificate file for this contact.

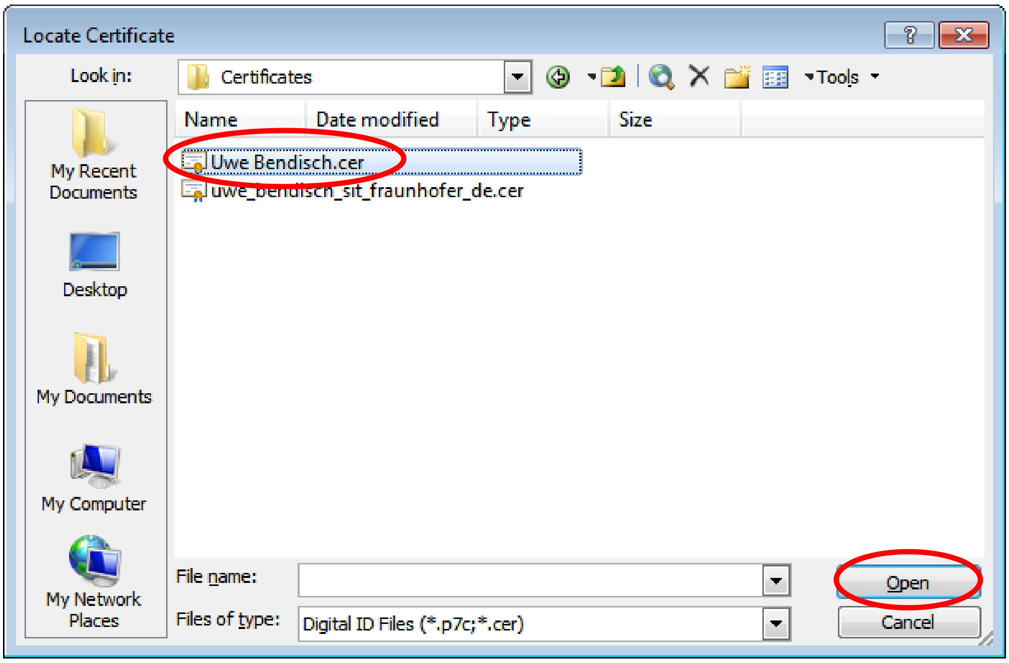
Certificates (Digital IDs):

Show social network updates in Outlook.

There are no items to show in this view.

Figure 72: Importing the Fraunhofer employee’s certificate into Outlook 2003

Now go to the directory where you saved the Fraunhofer employee’s certificate and select it. Click **Open** (see Figure 73).



Look in: Certificates

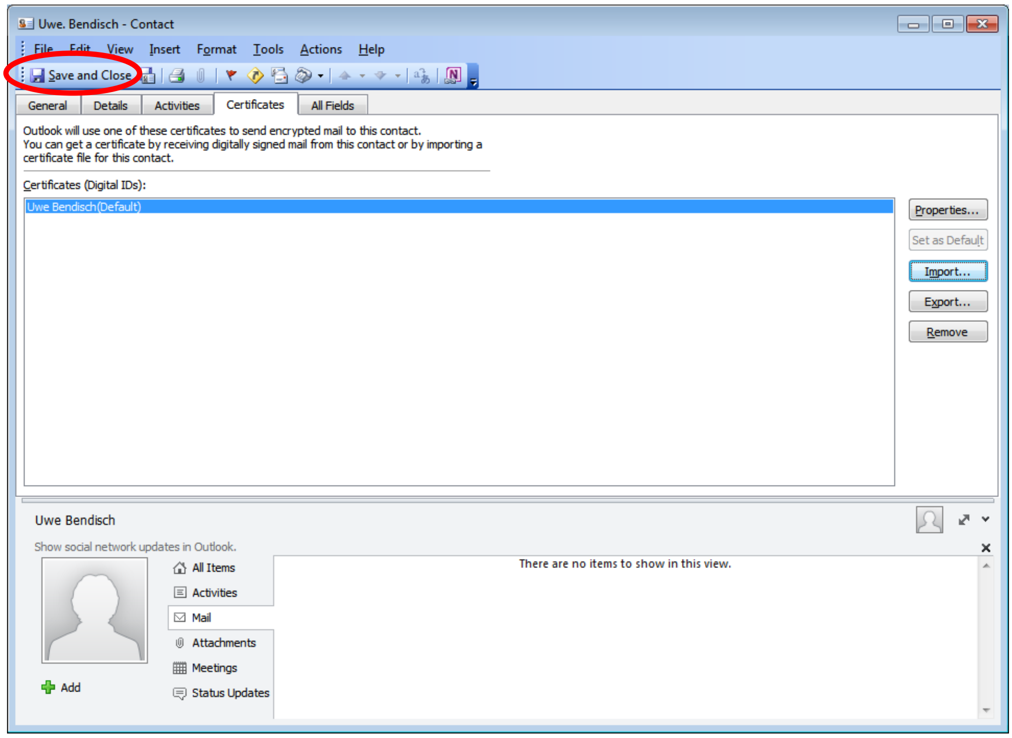
Uwe Bendisch.cer
uwe_bendisch_sit_fraunhofer_de.cer

File name:

Files of type: Digital ID Files (*.p7c;*.cer)

Figure 73: Selecting the Fraunhofer employee’s certificate

The certificate has now been added to the certificate store. Now click on **Save & Close** (see Figure 74).



Uwe. Bendisch - Contact

Outlook will use one of these certificates to send encrypted mail to this contact.
You can get a certificate by receiving digitally signed mail from this contact or by importing a certificate file for this contact.

Certificates (Digital IDs):

Uwe Bendisch(Default)

Uwe Bendisch

Show social network updates in Outlook.

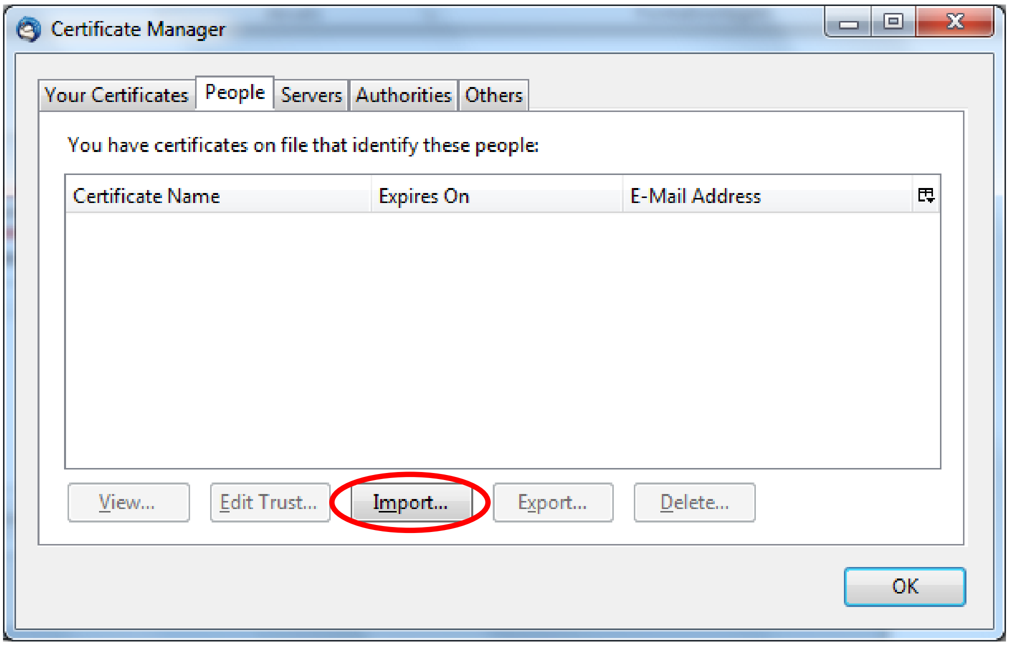
There are no items to show in this view.

Figure 74: Saving the certificate allocation in Outlook 2003

This concludes the process for integrating the Fraunhofer employee's certificate into Outlook 2003, meaning the certificate can be used for secure e-mail communication.

4.3.4 Incorporating a Fraunhofer employee's certificate into Mozilla Thunderbird

To embed the Fraunhofer employee's certificate into Mozilla Thunderbird, begin by opening the certificate manager found under **Extras → Options → Advanced → Certificates → View Certificates** and open up the **People** tab. Click on **Import** (see Figure 75).

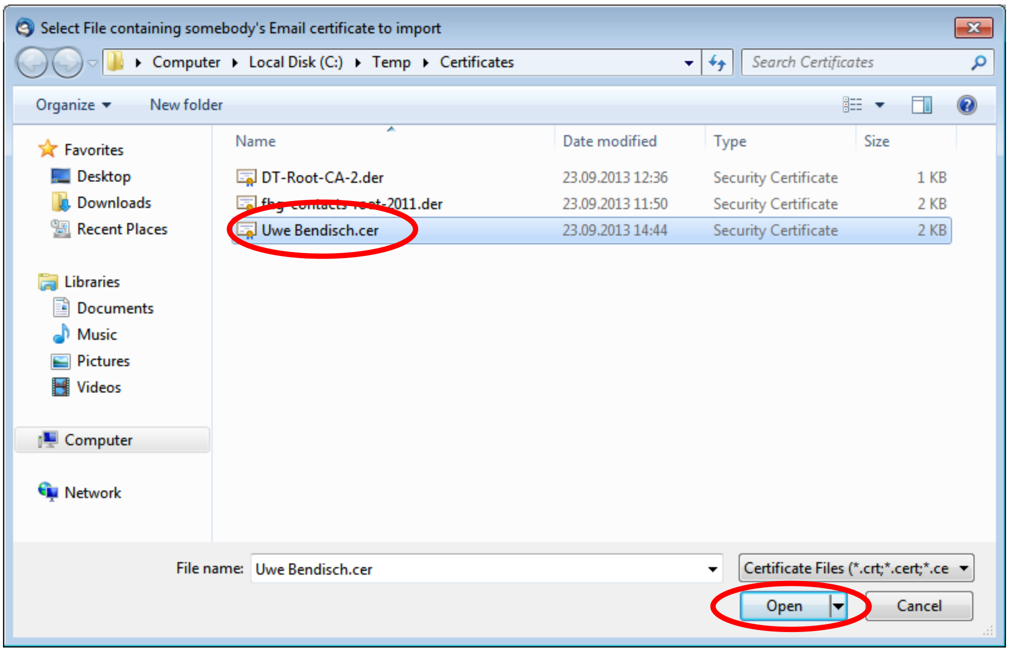


You have certificates on file that identify these people:

Certificate Name	Expires On	E-Mail Address

Figure 75: Importing a Fraunhofer employee’s certificate into Mozilla Thunderbird

Now go to the directory where you saved the Fraunhofer employee’s certificate and select it. Click **Open** (see Figure 76).



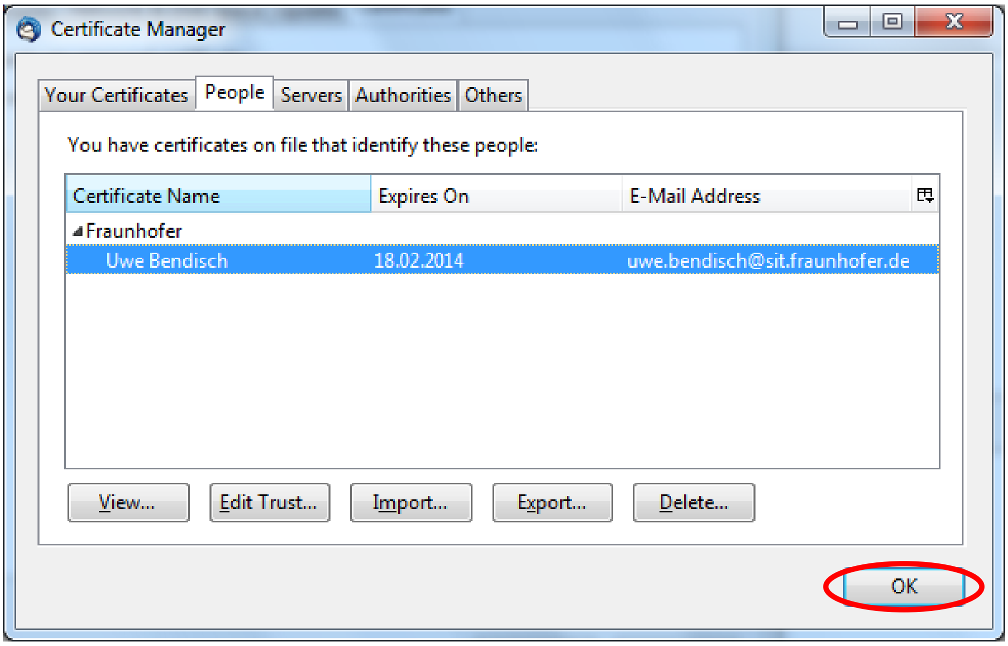
Name	Date modified	Type	Size
DT-Root-CA-2.der	23.09.2013 12:36	Security Certificate	1 KB
fhg-contacts-root-2011.der	23.09.2013 11:50	Security Certificate	2 KB
Uwe Bendisch.cer	23.09.2013 14:44	Security Certificate	2 KB

File name: Uwe Bendisch.cer

Certificate Files (*.crt;*.cert;*.ce

Figure 76: Selecting the Fraunhofer employee’s certificate

The certificate has now been added to the certificate store (see Figure 77), and the process to integrate the Fraunhofer employee's certificate into Thunderbird is complete. Close the certificate manager by clicking **OK**. The certificate can now be used for secure e-mail communication.



You have certificates on file that identify these people:

Certificate Name	Expires On	E-Mail Address
◢Fraunhofer		
Uwe Bendisch	18.02.2014	uwe.bendisch@sit.fraunhofer.de

Figure 77: Thunderbird certificate manager featuring the Fraunhofer employee's certificate.

4.4 Sending digitally signed and/or encrypted e-mails

Signed e-mails that you send use your personal certificate, and do not require recipients' certificates. Your e-mail client calculates a checksum from the text in your e-mail, and adds a digital signature to it using your certificate. The underlying mathematical process means the recipient is able to verify both the integrity of the e-mail (that it was not changed during transmission) and the authenticity of the sender (that the e-mail is indeed from you).

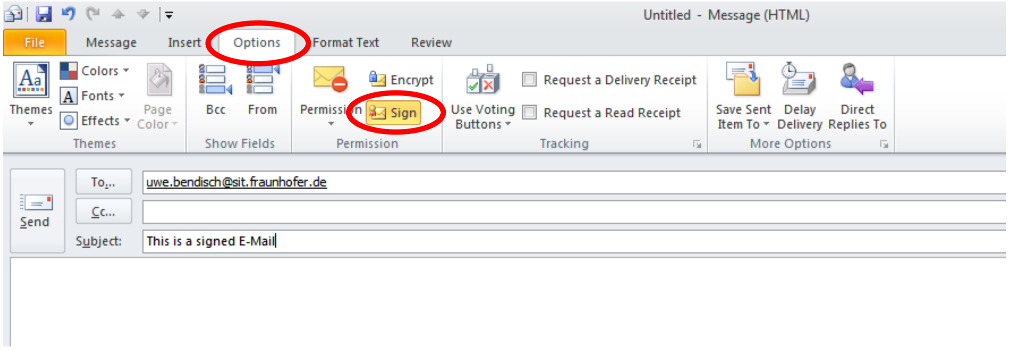
Encrypted e-mails that you send require the encryption certificates of all recipients. Using the encryption certificates, the message is encrypted in such a way that only the person in possession of the private key that goes with the encryption certificate can read it. This guarantees confidentiality.

It therefore follows that to send a signed and encrypted e-mail you require both your own personal certificate (sender's certificate) and the certificates of all the recipients of the e-mail.

The dialog windows and the steps in the process for sending signed and/or encrypted e-mails vary slightly depending on the e-mail client you use. For this reason the following subsections describe the process for different versions of Microsoft Outlook and Mozilla Thunderbird.

4.4.1 Sending digitally signed and/or encrypted e-mails using Microsoft Outlook 2010

Create a new e-mail. You have the option to digitally sign the e-mail when composing it by clicking on the **Sign** symbol in the **Options** tab (see Figure 78).

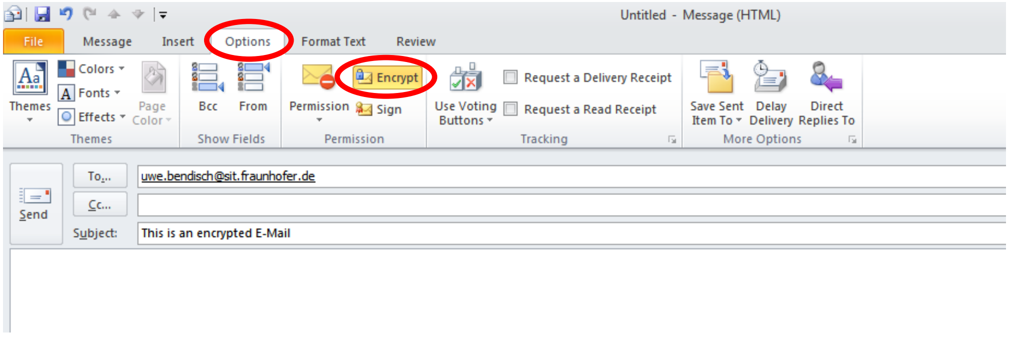


To...: uwe.bendisch@sit.fraunhofer.de

Subject: This is a signed E-Mail

Figure 78: Adding a digital signature to an e-mail in Outlook 2010

To encrypt an e-mail, click the **Encryption** symbol in the **Options** tab (see Figure 79).



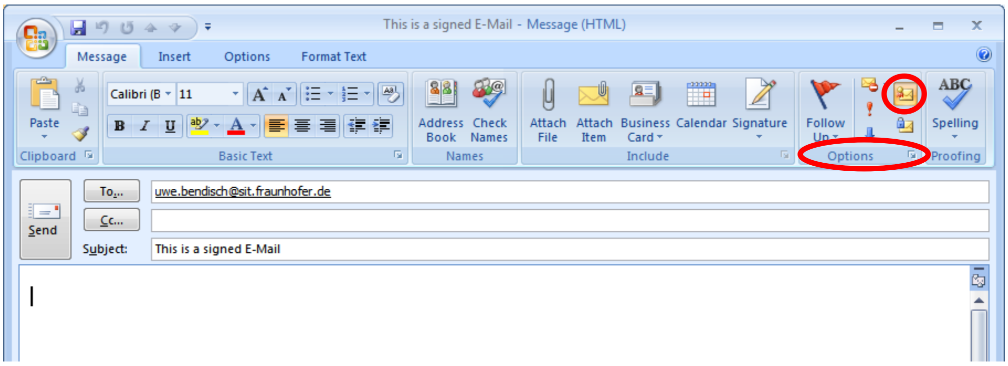
To...: uwe.bendisch@sit.fraunhofer.de

Subject: This is an encrypted E-Mail

Figure 79: Encrypting an e-mail in Outlook 2010

4.4.2 Sending digitally signed and/or encrypted e-mails using Microsoft Outlook 2007

Create a new e-mail. You have the option to digitally sign the e-mail when composing it by clicking on the **Sign** symbol found in the **Options** section of the menu ribbon under the **Message** tab (see Figure 80).


This is a signed E-Mail - Message (HTML)

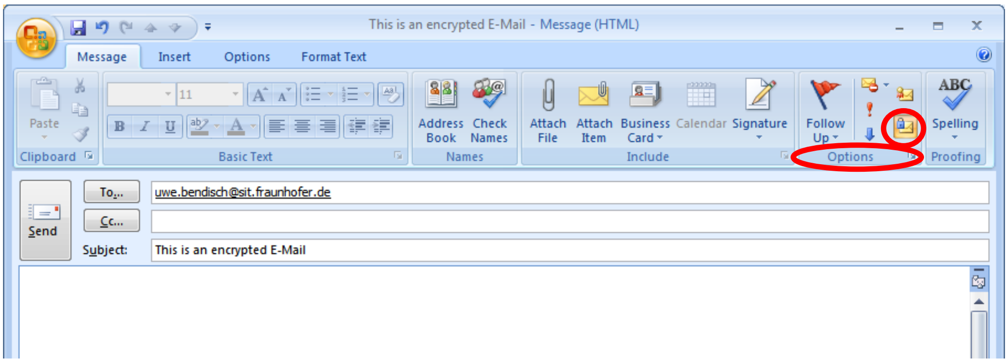
To... uwe.bendisch@sit.fraunhofer.de

Cc...

Subject: This is a signed E-Mail

Figure 80: Adding a digital signature to an e-mail in Outlook 2007

To encrypt an e-mail, click the **Encryption** symbol in the **Options** section of the M**essage** tab (see Figure 81).


This is an encrypted E-Mail - Message (HTML)

To... uwe.bendisch@sit.fraunhofer.de

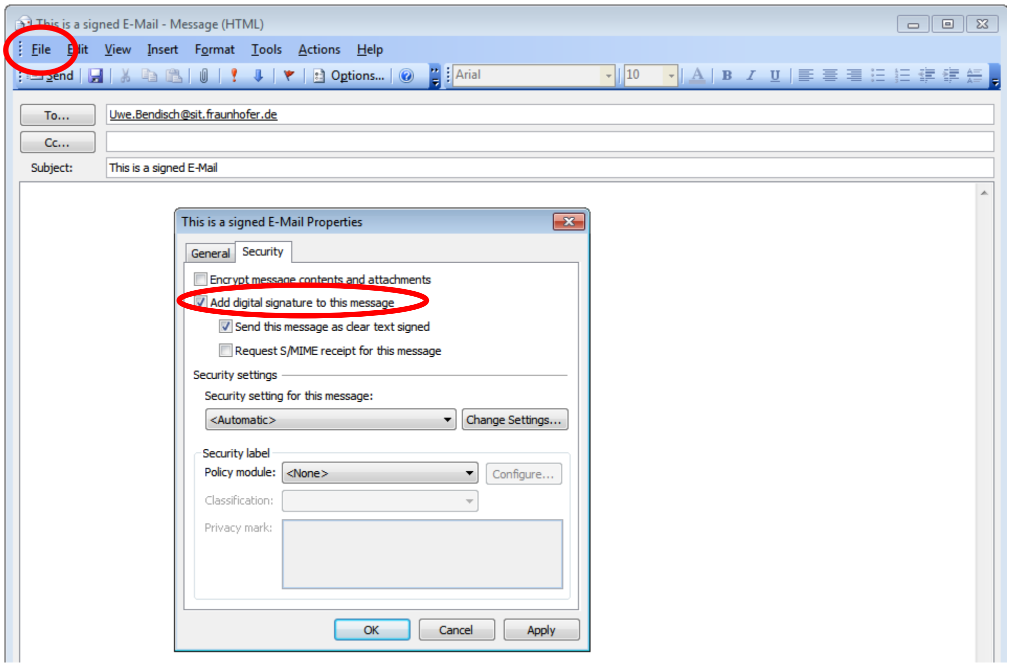
Cc...

Subject: This is an encrypted E-Mail

Figure 81: Encrypting an e-mail in Outlook 2007

4.4.3 Sending digitally signed and/or encrypted e-mails using Microsoft Outlook 2003

Create a new e-mail. You have the option to digitally sign the e-mail when composing it by selecting the option **Add digital signature to this message** in the message security properties, found under **File → Properties** in the **Security** tab (see Figure 82).



This is a signed E-Mail - Message (HTML)

To... Uwe.Bendisch@sit.fraunhofer.de

Cc...

Subject: This is a signed E-Mail

This is a signed E-Mail Properties

General | Security

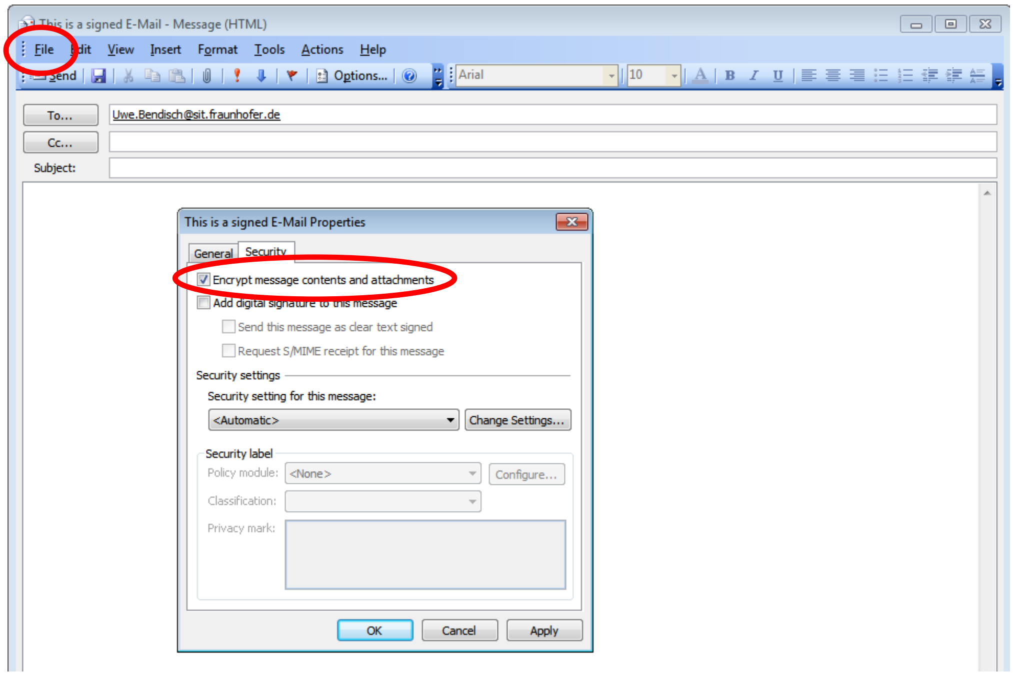
☐ Encrypt message contents and attachments
☑ Add digital signature to this message
☑ Send this message as clear text signed
☐ Request S/MIME receipt for this message

Security settings
Security setting for this message: <Automatic>

Security label
Policy module: <None>
Classification:
Privacy mark:

Figure 82: Adding a digital signature to an e-mail in Outlook 2003

To encrypt the e-mail, select the **Encrypt message contents and attachments** option under the **Security** tab, found under **File → Properties** for the e-mail (see Figure 83).



This is a signed E-Mail - Message (HTML)

To... Uwe.Bendisch@sit.fraunhofer.de

Cc...

Subject:

This is a signed E-Mail Properties

General | Security

☑ Encrypt message contents and attachments
☐ Add digital signature to this message
☐ Send this message as clear text signed
☐ Request S/MIME receipt for this message

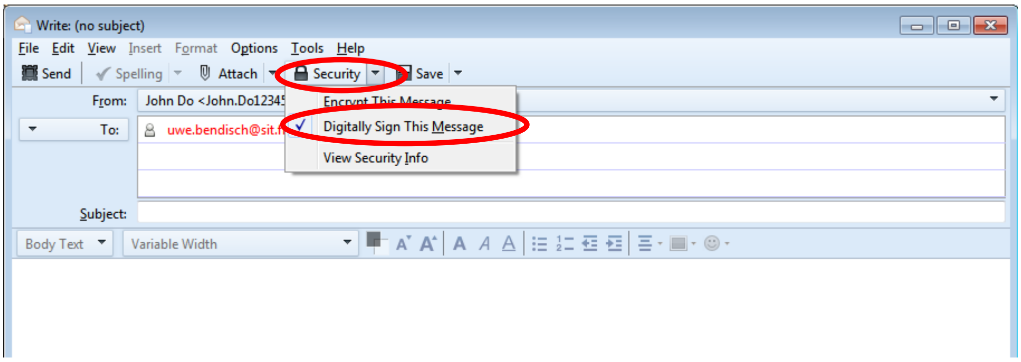
Security settings
Security setting for this message: <Automatic>

Security label
Policy module: <None>
Classification:
Privacy mark:

Figure 83: Encrypting an e-mail Outlook 2003

4.4.4 Sending digitally signed and/or encrypted e-mails using Mozilla Thunderbird

Create a new e-mail. You have the option to digitally sign the e-mail when composing it by selecting the **Digitally Sign This Message** option under the **Security** header in the message Menu (see Figure 84). Open the S/MIME options by clicking on the little arrow next to the menu item.

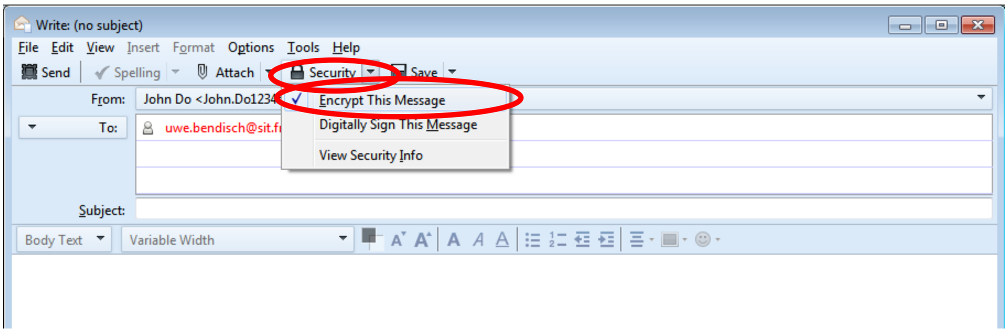


From: John Do <John.Do12345

To: uwe.bendisch@sit.f

Figure 84: Adding a digital signature to an e-mail in Mozilla Thunderbird

To encrypt an e-mail, select the **Encrypt This Message** option under the **Security** header (see Figure 85).



From: John Do <John.Do1234

To: uwe.bendisch@sit.f

Figure 85: Encrypting an e-mail in Mozilla Thunderbird

5 Revoking a personal certificate

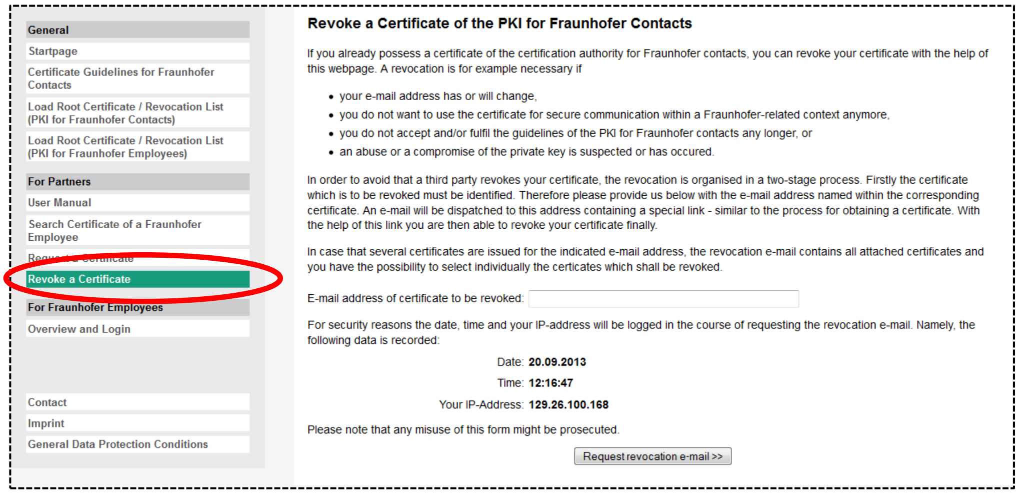
If you are already in possession of a certificate issued by the Certification Authority for Fraunhofer Contacts and wish to revoke it, you can request a revocation at https://contacts.pki.fraunhofer.de. Revoking a certificate may be necessary if:

- your e-mail address has changed or will change,
- you do not want to use the certificate for secure communication within a Fraunhofer-related context anymore,
- you no longer accept and/or fulfil the guidelines of the PKI for Fraunhofer Contacts any longer, or
- (especially if) abuse or compromise of the private key is suspected or has occurred.

In order to prevent a third party from revoking your certificate, revocation is set up as a two-stage process. First, the certificate that is to be revoked must be identified. Please do so by providing us with the e-mail address named in the certificate. An e-mail will be dispatched to this address containing a special link – similar to the process for obtaining a certificate. This link then enables you to revoke the certificate yourself.

5.1 Requesting the revocation of a personal certificate by e-mail

Please go to https://contacts.pki.fraunhofer.de and select **Revoke a Certificate** in the **For Partners** section of the menu (see Figure 86).


General
Startpage
Certificate Guidelines for Fraunhofer Contacts
Load Root Certificate / Revocation List (PKI for Fraunhofer Contacts)
Load Root Certificate / Revocation List (PKI for Fraunhofer Employees)
For Partners
User Manual
Search Certificate of a Fraunhofer Employee
Request a Certificate
Revoke a Certificate
For Fraunhofer Employees
Overview and Login
Contact
Imprint
General Data Protection Conditions

Revoke a Certificate of the PKI for Fraunhofer Contacts

If you already possess a certificate of the certification authority for Fraunhofer contacts, you can revoke your certificate with the help of this webpage. A revocation is for example necessary if

- your e-mail address has or will change,
- you do not want to use the certificate for secure communication within a Fraunhofer-related context anymore,
- you do not accept and/or fulfil the guidelines of the PKI for Fraunhofer contacts any longer, or
- an abuse or a compromise of the private key is suspected or has occured.

In order to avoid that a third party revokes your certificate, the revocation is organised in a two-stage process. Firstly the certificate which is to be revoked must be identified. Therefore please provide us below with the e-mail address named within the corresponding certificate. An e-mail will be dispatched to this address containing a special link - similar to the process for obtaining a certificate. With the help of this link you are then able to revoke your certificate finally.

In case that several certificates are issued for the indicated e-mail address, the revocation e-mail contains all attached certificates and you have the possibility to select individually the certicates which shall be revoked.

E-mail address of certificate to be revoked:

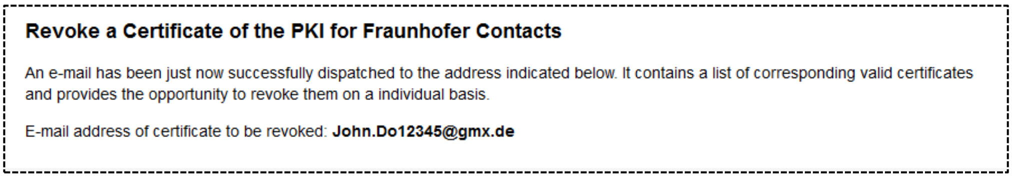
For security reasons the date, time and your IP-address will be logged in the course of requesting the revocation e-mail. Namely, the following data is recorded:

Date: **20.09.2013**
Time: **12:16:47**
Your IP-Address: **129.26.100.168**

Please note that any misuse of this form might be prosecuted.

Figure 86: Requesting the revocation of a certificate

Now enter the e-mail address that is assigned to your personal certificate into the **E-mail address of certificate to be revoked** field. Then click **Request revocation e-mail**. Provided there are valid certificates available that were assigned to the e-mail address you entered, you will receive a message informing you that a list of all valid certificates assigned to the e-mail address has been sent out along with the option to revoke them (see Figure 87).



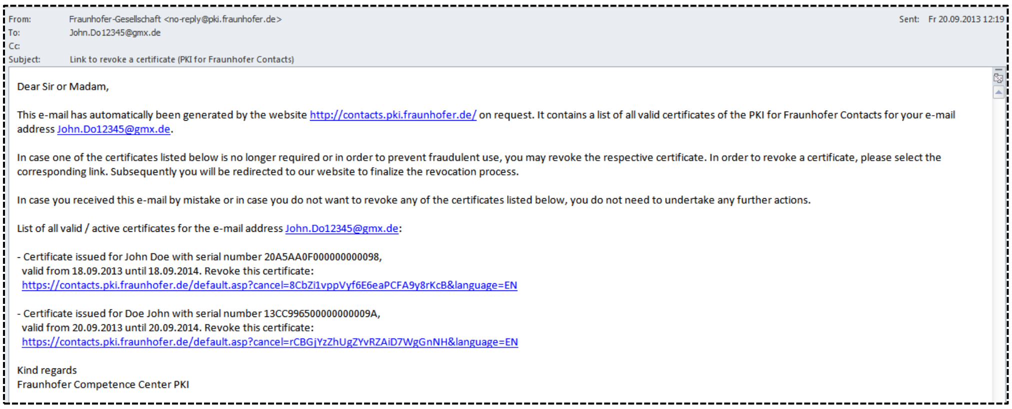
Revoke a Certificate of the PKI for Fraunhofer Contacts

An e-mail has been just now successfully dispatched to the address indicated below. It contains a list of corresponding valid certificates and provides the opportunity to revoke them on a individual basis.

E-mail address of certificate to be revoked: **John.Do12345@gmx.de**

Figure 87: Message indicating that the user's request for revocation was successful

If this is not the case, a message appears informing you that an e-mail has not been sent. This concludes the process for requesting a revocation e-mail. You must now wait for the automatically generated revocation e-mail to appear in your inbox before you can revoke the certificate (see Figure 88). This e-mail will arrive after a short time.



From: Fraunhofer-Gesellschaft <no-reply@pki.fraunhofer.de>
To: John.Do12345@gmx.de
Cc:
Subject: Link to revoke a certificate (PKI for Fraunhofer Contacts)
Sent: Fr 20.09.2013 12:19

Dear Sir or Madam,

This e-mail has automatically been generated by the website http://contacts.pki.fraunhofer.de/ on request. It contains a list of all valid certificates of the PKI for Fraunhofer Contacts for your e-mail address John.Do12345@gmx.de.

In case one of the certificates listed below is no longer required or in order to prevent fraudulent use, you may revoke the respective certificate. In order to revoke a certificate, please select the corresponding link. Subsequently you will be redirected to our website to finalize the revocation process.

In case you received this e-mail by mistake or in case you do not want to revoke any of the certificates listed below, you do not need to undertake any further actions.

List of all valid / active certificates for the e-mail address John.Do12345@gmx.de:

- Certificate issued for John Doe with serial number 20A5AA0F000000000098,
  valid from 18.09.2013 until 18.09.2014. Revoke this certificate:
  https://contacts.pki.fraunhofer.de/default.asp?cancel=8CbZi1vppVyf6E6eaPCFA9y8rKcB&language=EN

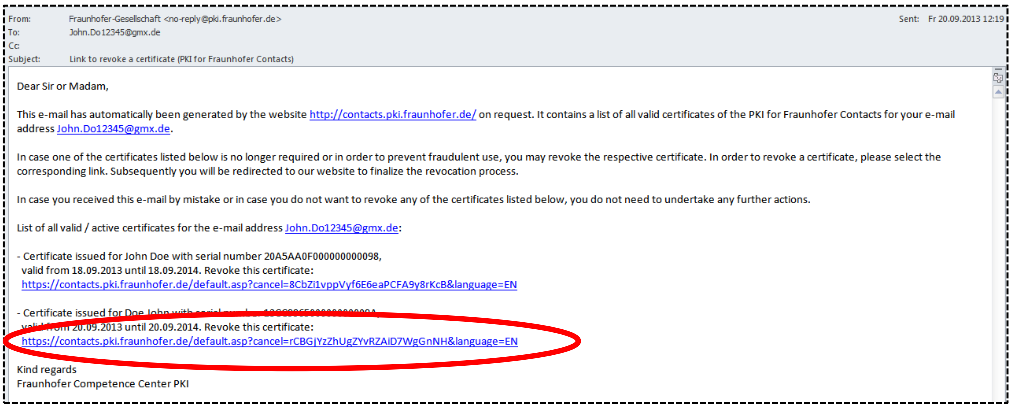
- Certificate issued for Doe John with serial number 13CC996500000000009A,
  valid from 20.09.2013 until 20.09.2014. Revoke this certificate:
  https://contacts.pki.fraunhofer.de/default.asp?cancel=rCBGjYzZhUgZYvRZAiD7WgGnNH&language=EN

Kind regards
Fraunhofer Competence Center PKI

Figure 88: Example of a revocation e-mail for revoking a certificate

5.2 Permanently revoking a personal certificate using the revocation e-mail

In instances where several certificates have been issued for the e-mail address given, the revocation e-mail will list all relevant certificates that are still valid and give you the opportunity to individually select which certificates are to be revoked. To permanently revoke a certificate listed in the e-mail, click on the relevant link in the e-mail or copy it into the address bar in your browser (see Figure 89).



From: Fraunhofer-Gesellschaft <no-reply@pki.fraunhofer.de>
To: John.Do12345@gmx.de
Cc:
Subject: Link to revoke a certificate (PKI for Fraunhofer Contacts)
Sent: Fr 20.09.2013 12:19

Dear Sir or Madam,

This e-mail has automatically been generated by the website http://contacts.pki.fraunhofer.de/ on request. It contains a list of all valid certificates of the PKI for Fraunhofer Contacts for your e-mail address John.Do12345@gmx.de.

In case one of the certificates listed below is no longer required or in order to prevent fraudulent use, you may revoke the respective certificate. In order to revoke a certificate, please select the corresponding link. Subsequently you will be redirected to our website to finalize the revocation process.

In case you received this e-mail by mistake or in case you do not want to revoke any of the certificates listed below, you do not need to undertake any further actions.

List of all valid / active certificates for the e-mail address John.Do12345@gmx.de:

- Certificate issued for John Doe with serial number 20A5AA0F000000000098,
  valid from 18.09.2013 until 18.09.2014. Revoke this certificate:
  https://contacts.pki.fraunhofer.de/default.asp?cancel=8CbZi1vppVyf6E6eaPCFA9y8rKcB&language=EN

- Certificate issued for Doe John with serial number 13CC996500000000009A,
  valid from 20.09.2013 until 20.09.2014. Revoke this certificate:
  https://contacts.pki.fraunhofer.de/default.asp?cancel=rCBGjYzZhUgZYvRZAiD7WgGnNH&language=EN

Kind regards
Fraunhofer Competence Center PKI

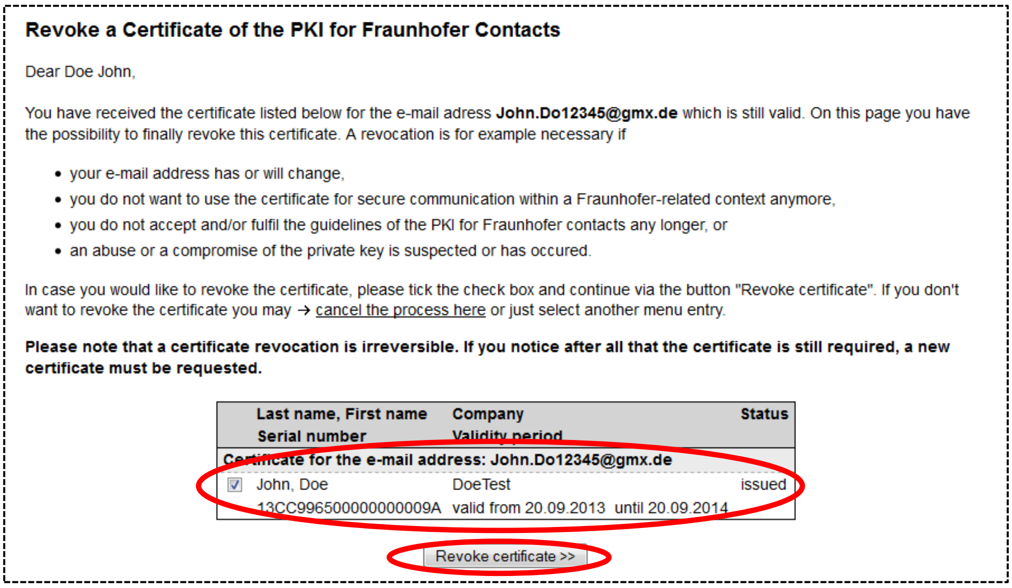
Figure 89: Selecting a certificate you wish to revoke from the list provided in the revocation e-mail

The link takes you to a special *PKI Contacts* web page that will lead you through the certificate revocation process (see Figure 90). Read through the text on the web page carefully, making sure you understand that

- regardless of whether the revocation takes place, you should **not** destroy the private key that goes with the certificate, as without it you will be unable to read i.e. decrypt e-mails that were encrypted for you using the certificate in question. For this reason you should if applicable retain a backup copy of your certificate along with its private key and keep it in a safe place (such as an external hard drive). Alternatively, both certificate and private key are still available in the certificate store of the browser you used to request the certificate in the first place. You can use the method described in Chapter 3 to export it from here.

- it is not possible to undo a revocation. If you realize after revoking a certificate that you need it after all, you will have to request a new (different) certificate.

To revoke the certificate in question, please check the tick box by the selected certificate entry and click **Revoke certificate** (see Figure 90).



Revoke a Certificate of the PKI for Fraunhofer Contacts

Dear Doe John,

You have received the certificate listed below for the e-mail adress **John.Do12345@gmx.de** which is still valid. On this page you have the possibility to finally revoke this certificate. A revocation is for example necessary if

- your e-mail address has or will change,
- you do not want to use the certificate for secure communication within a Fraunhofer-related context anymore,
- you do not accept and/or fulfil the guidelines of the PKI for Fraunhofer contacts any longer, or
- an abuse or a compromise of the private key is suspected or has occured.

In case you would like to revoke the certificate, please tick the check box and continue via the button "Revoke certificate". If you don't want to revoke the certificate you may → cancel the process here or just select another menu entry.

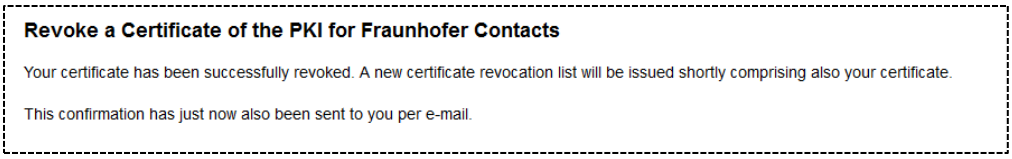
Please note that a certificate revocation is irreversible. If you notice after all that the certificate is still required, a new certificate must be requested.

	Last name, First name Serial number	Company Validity period	Status
Certificate for the e-mail address: John.Do12345@gmx.de			
☑	John, Doe 13CC996500000000009A	DoeTest valid from 20.09.2013 until 20.09.2014	issued

Figure 90: Confirming the selection of a certificate that is to be revoked

You will now receive a message informing you that the revocation was carried out and that a new revocation list will be published shortly (see Figure 91). You will also receive an automatic e-mail informing you that the revocation has taken place (see Figure 92). This successfully concludes the revocation process.

Note: The revocation list containing the serial number of the certificate that has been revoked will appear on the PKI for Fraunhofer Contacts website no later than 30 minutes after a successful revocation.

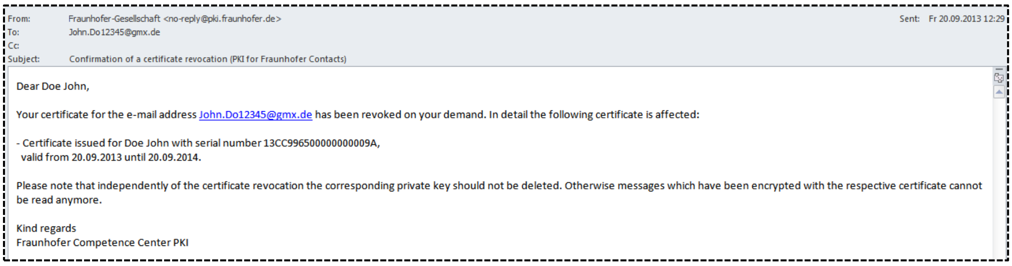


Revoke a Certificate of the PKI for Fraunhofer Contacts

Your certificate has been successfully revoked. A new certificate revocation list will be issued shortly comprising also your certificate.

This confirmation has just now also been sent to you per e-mail.

Figure 91: Confirmation that your personal certificate has been revoked



From: Fraunhofer-Gesellschaft <no-reply@pki.fraunhofer.de>
Sent: Fr 20.09.2013 12:29
To: John.Do12345@gmx.de
Cc:
Subject: Confirmation of a certificate revocation (PKI for Fraunhofer Contacts)

Dear Doe John,

Your certificate for the e-mail address John.Do12345@gmx.de has been revoked on your demand. In detail the following certificate is affected:

- Certificate issued for Doe John with serial number 13CC996500000000009A,
  valid from 20.09.2013 until 20.09.2014.

Please note that independently of the certificate revocation the corresponding private key should not be deleted. Otherwise messages which have been encrypted with the respective certificate cannot be read anymore.

Kind regards
Fraunhofer Competence Center PKI

Figure 92: E-mail confirming that your personal certificate has been revoked